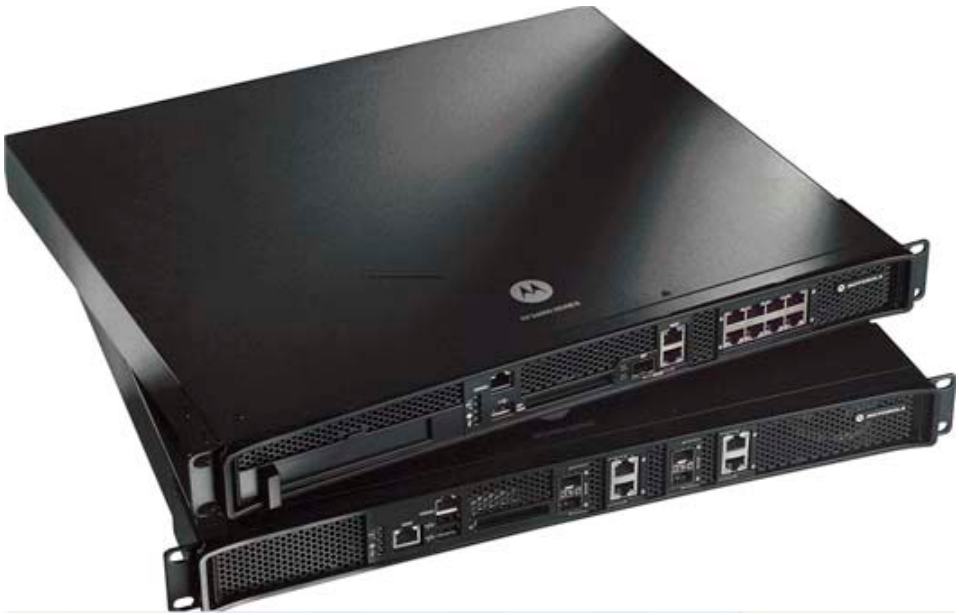
MOTOROLA

Motorola RFS Series Wireless LAN Switches

WiNG CLI Reference Guide



© 2009 Motorola, Inc. All rights reserved.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Symbol is a registered trademark of Symbol Technologies, Inc. All other product or service names are the property of their respective owners.

About This Guide

This *Motorola RF Switch CLI Reference Guide* and contains the following sections:

- *Who Should Use this Guide*
- *How to Use this Guide*
- *Conventions Used in this Guide*
- *Motorola Service Information*
- *Motorola, Inc. End-User License Agreement*

Who Should Use this Guide

The *Motorola RF Switch CLI Reference Guide* is intended for administrators responsible for implementing, configuring, and maintaining a RFS6000 or RFS7000 model switch using the switch's *command line interface* (CLI). It also serves as a reference for configuring/modifying system settings. The administrator should be familiar with wireless technologies, networking concepts, Ethernet concepts, IP addressing and SNMP.

To avoid confusion amongst RFS6000 and RFS7000 CLI users, generic examples are used throughout this guide. These examples are relevant to each switch.

Example

```
RFSwitch>cluster-cli enable
RFSwitch>
```

The syntax, parameters and descriptions within this guide can also be used generically for a RFS6000 and RFS7000 model switch. However, some subtle differences do exist amongst these baselines. These differences are strongly noted within the specific commands impacted. When these differences are noted, the options available to each switch baseline are described in detail.

How to Use this Guide

This guide will help you implement, configure, and administer the switch and associated network elements. This guide is organized into the following sections:

Chapter	***Jump to this section if you want to...***
Chapter 1, "Introduction"	Review the overall feature-set of the switch, as well as the many configuration options available.
Chapter 2, "Common Commands"	Understand the commands common amongst many contexts and instance contexts within the switch CLI.
Chapter 3, "User Exec Commands"	Summarize the User Exec commands within the switch CLI.
Chapter 4, "Privileged Exec Commands"	Review the Priv Exec commands within the switch CLI.
Chapter 5, "Global Configuration Commands"	Understand the Global Config commands within the switch CLI.
Chapter 6, "Crypto-isakmp Instance"	Review the **(crypto-isakmp)** commands within the switch CLI.
Chapter 7, "Crypto-group Instance"	Understand the **(crypto-group)** commands within the switch CLI.
Chapter 8, "Crypto-peer Instance"	Summarize the **(crypto-peer)** commands within the switch CLI.
Chapter 9, "Crypto-ipsec Instance"	Review the **(crypto-ipsec)** commands within the switch CLI.

Chapter	***Jump to this section if you want to...***
Chapter 10, "Crypto-map Instance"	Understand the **(crypto-map)** commands within the switch CLI.
Chapter 11, "Crypto-trustpoint Instance"	Summarize the **(crypto trustpoint)** commands within the switch CLI.
Chapter 12, "Interface Instance"	Understand the **(config-if)** commands within the switch CLI.
Chapter 13, "Spanning tree-mst Instance"	Summarize the **(config-mst)** instance commands within the switch CLI.
Chapter 14, "Extended ACL Instance"	Review the **(config-ext-nacl)** commands within the switch CLI.
Chapter 15, "Standard ACL Instance"	Understand the **(config-std-nacl**) commands within the switch CLI.
Chapter 16, "Extended MAC ACL Instance"	Review the **(config-ext-macl)** commands within the switch command line.
Chapter 17, "DHCP Server Instance"	Understand the **(config-dhcp-pool)** commands within the switch command line.
Chapter 18, "DHCP Class Instance"	Review the **(config-dhcp-class)** instance commands within the switch CLI.
Chapter 19, "Radius Server Instance"	Summarize the **(config-radsrv)** instance commands within the switch CLI.
Chapter 20, "Wireless Instance"	Understand the **(config-wireless)** instance commands within the switch CLI.
Chapter 21, "RTLS Instance"	Review the **(config-rtls)** instance commands within the switch CLI.
Chapter 22, "ESPI Instance"	Review the **(config-rtls-espi)** instance commands within the switch CLI
Chapter 23, "RFID Instance"	Review the **(config-rtls-rfid)** instance commands within the switch CLI

Chapter	***Jump to this section if you want to...***
Chapter 24, "SOLE Instance"	Review the **`(config-rtls-sole)`** instance commands within the switch CLI
Chapter 25, "Smart RF Instance"	Review the **`(config-wireless-smart-rf)`** instance commands within the switch CLI
Chapter 26, "Role Instance"	Review the **`(config-role)`** instance commands within the switch CLI

Conventions Used in this Guide

This section describes the following topics:

- *Annotated Symbols*
- *Notational Conventions*

Annotated Symbols

The following document conventions are used in this document:



NOTE: Indicates tips or special requirements.



CAUTION: Indicates conditions that can cause equipment damage or data loss.



SWITCH NOTE: Indicates caveats unique to a RFS6000 or RFS7000 model switch.



WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Understanding Command Syntax

command / keyword — The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.

For example, the command,

```
RFSwitch>show wlan 1
```

is documented as

```
show wlan <idx>
```

where:

- show – The command
- wlan – The keyword

<variable> — Variables are described with a short description enclosed within a '<' and a '>' pair.

For example, the command,

```
RFSwitch>show wlan 1
```

is documented as

```
show wlan <idx>
```

where:

- show – The command – Display information.
- wlan – The keyword – The wlan
- <idx> – The variable – WLAN Index value.

| The pipe symbol. This is used to separate the variables/keywords in a list.

For example, the command

```
RFSwitch> show .....
```

is documented as

```
show [autoinstall|banner|ip|ldap|......]
```

where:

- set – The command
- [autoinstall|banner|ip|ldap|.....] – Indicates the different commands that can be combined with the show command. However, only one of the above list can be used at a time.

```
show autoinstall ...
show banner ...
show ip ...
show ldap ...
```

[ ] Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '|' (pipe) symbol.

For example, the command

```
RFSwitch> clear ...
```

is documented as

```
clear [crypto|mobility|spanning-tree]
```

where:

- clear – The command
- [crypto|mobility|spanning-tree] – Indicates that three keywords are available for this command and only one can be used at a time

{ }

Any command/keyword/variable or a combination of them inside a '*{*' & '*}*' pair is optional. All optional commands follow the same conventions as listed above. However they are displayed italicized.

For example, the command

```
RFSwitch> show autoinstall ....
```

is documented as

```
show autoinstall {status}
```

Here:

- show autostatus– The command. This command can also be used as

  ```
  show autostatus
  ```

- *{status}* – The optional keyword status. The command can also be extended as

  ```
  show autoinstall status
  ```

Here the keyword *status* is optional.

<values>

Values to be entered as shown in Blue.

For example, the command

```
RFSwitch>show wlan 1
```

is documented as

```
show wlan <idx>
```

This command's parameter <idx> is described as under:

"<idx> – <idx> (1-8) is the Wlan Index."

Motorola Service Information

Use the Motorola Support Center as the primary contact for any technical problem, question, or support issue involving Motorola products. Motorola Support Center responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements:

Telephone (North America): 1-800-653-5350

Telephone (International): +1-631-738-6213

Fax: (631) 738-5410

Email: *emb.support@motorola.com*

When contacting Motorola Support Center, please provide the following information:

- Serial number of the unit.
- Model number or product name.
- Software type and version number.

Customer Support Website

Comprehensive on-line support is available at *http://www.symbol.com/support/* . Registration is free and a variety of services can be linked through this Web portal.

Product Sales and Product Information

Motorola, Inc.

One Motorola Plaza

Holtsville, New York 11742-1300

Tel: 1-631-738-2400 or 1-800-722-6234

Fax: 1-631-738-5990

General Information

For general information, contact Motorola at:

Telephone (North America): 1-800-722-6234

Telephone (International): +1-631-738-5200

Website: *http://www.motorola.com*

Motorola, Inc.
End-User License Agreement

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE DESCRIBED IN THIS DOCUMENT, YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT"). LICENSEE'S USE OR CONTINUED USE OF THE DOWNLOADED OR INSTALLED MATERIALS SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUTE THE INSTALLATION PROCESS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO AND EXPRESSLY CONTINGENT UPON THESE TERMS. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY, ANOTHER PERSON OR ANY OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THAT COMPANY, PERSON OR ENTITY.

1. LICENSE GRANT. Subject to the terms of this Agreement, Motorola, Inc. and/or its subsidiaries ("Licensor") hereby grants Licensee a limited, personal, non-sublicensable, non transferable, non-exclusive license to use the software that Licensee is about to download or install and the documentation that accompanies it (collectively, the "Software") for Licensee's personal use in connection with hardware produced by Licensor and only in accordance with the accompanying documentation. Licensee may download, install and use the Software only on a single computer. Licensee may make one copy of the Software (excluding any documentation) for backup purposes, provided that copyright and other restricted rights notices of Licensor and its suppliers are reproduced exactly.
2. LICENSE RESTRICTIONS. Except as expressly permitted by this Agreement, Licensee shall not, nor permit anyone else to, directly or indirectly: (i) copy (except for one backup copy), modify, distribute or create derivative works based upon the Software; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or structure, sequence and organization of the Software; or (iii) rent, lease, or use the Software for timesharing or service bureau purposes, or otherwise use the Software for any commercial purpose/on behalf of any third party. Licensee shall maintain and not remove or obscure any proprietary notices on the Software, and shall reproduce such notices exactly on all permitted copies of the Software. All title, ownership rights, and intellectual property rights in and to the Software, and any copies or portions thereof, shall remain in Licensor and its suppliers or licensors. Licensee understands that Licensor may modify or discontinue offering the Software at any time. The Software is protected by the copyright laws of the United States and international copyright treaties. The Software is licensed, not sold. This Agreement does not give Licensee any rights not expressly granted herein.

3. INTELLECTUAL PROPERTY; CONTENT. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Software), and any copies you are permitted to make herein are owned by Licensor or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. As a condition to Licensee's use of the Software, Licensee represents, warrants and covenants that Licensee will not use the Software: (i) to infringe the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance or regulation; (iii) to disseminate information or materials in any form or format ("Content") that are harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or (iv) to disseminate any software viruses or any other computer code, files or programs that may interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. Licensee, not Licensor, remains solely responsible for all Content that Licensee uploads, posts, e-mails, transmits, or otherwise disseminates using, or in connection with, the Software.
4. FEES; SUPPORT AND UPGRADES. Licensor may, at Licensor's sole option, provide support services related to the Software ("Support Services"). Nothing in this Agreement grants Licensee any right to receive any Support Services. Use of any Support Services provided is governed by the Licensor policies and programs described in the user manual, in "online" documentation, and/or in other Licensor-provided materials or support agreements. Any supplemental software code provided to you as part of any Support Services shall be considered part of the Software and subject to the terms and conditions of this EULA. With respect to technical information you provide to Licensor as part of any Support Services, Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies Licensee.
5. TERMINATION. Either party may terminate this Agreement at any time, with or without cause, upon written notice. Any termination of this Agreement shall also terminate the licenses granted hereunder. Upon termination of this Agreement for any reason, Licensee shall return all copies of the Software to Licensor, or destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Software, and shall so certify to Licensor that such actions have occurred. Sections 2-13 shall survive termination of this Agreement.

6. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Licensor and its suppliers provide the Software and any (if any) Support Services AS IS AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NONINFRINGEMENT WITH REGARD TO THE SOFTWARE. THE ENTIRE RISK AS TO THE QUALITY OF OR ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE AND SUPPORT SERVICES, IF ANY, REMAINS WITH LICENSEE.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY GENERAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF LICENSOR OR ANY SUPPLIER, AND EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that Licensee might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Licensor and any of its suppliers under any provision of this Agreement and Licensee's exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by Licensee for the Software or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

9. INDEMNITY. Licensee agrees that Licensor shall have no liability whatsoever for any use Licensee makes of the Software. Licensee shall indemnify and hold harmless Licensor from any claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from Licensee's use of the Software as well as from Licensee's failure to comply with any term of this Agreement.
10. FAULT TOLERANCE. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale in on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, or weapons systems, in which the failure of the Software could lead directly or indirectly to death, personal injury, or physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.
11. U.S. GOVERNMENT LICENSE RIGHTS. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. Software provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227- 7013 (OCT 1988), as applicable. The "Manufacturer" for purposes of these regulations is Motorola, Inc., One Symbol Plaza, Holtsville, NY 11742.
12. EXPORT RESTRICTIONS. Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Software in violation of any such restrictions, laws or regulations. By downloading or using the Software, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.
13. MISCELLANEOUS. Licensee may not sublicense, assign, or transfer this Agreement, or its rights or obligations hereunder, without the prior written consent of Licensor. Any attempt to otherwise sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is null and void. Licensor may assign this Agreement in its sole discretion. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorized representative of such party and no failure or delay in enforcing any right will be deemed a

waiver. This Agreement shall be governed by the laws of the State of New York without regard to the conflicts of law provisions thereof. The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Unless waived by Licensor for a particular instance, any action or proceeding arising out of this Agreement must be brought exclusively in the state or federal courts of New York and Licensee hereby consents to the jurisdiction of such courts for any such action or proceeding. This Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof. The prevailing party in any action arising out of this Agreement shall be entitled to costs and attorneys' fees.

Contents

Chapter 1. Introduction

1.1 CLI Overview 1-2
1.2 Getting Context Sensitive Help 1-5
1.3 Using the No and Default Command Forms 1-7
1.3.1 Basic Conventions 1-7
1.4 Using CLI Editing Features and Shortcuts 1-8
1.4.1 Moving the Cursor on the Command Line 1-8
1.4.2 Completing a Partial Command Name 1-10
1.4.3 Deleting Entries 1-11
1.4.4 Re-displaying the Current Command Line 1-11
1.4.5 Command Output pagination 1-11
1.4.6 Transposing Mistyped Characters 1-12
1.4.7 Controlling Capitalization 1-12

Chapter 2. Common Commands

2.1 Common Commands 2-1
2.1.1 clrscr 2-2
2.1.2 exit 2-3
2.1.3 help 2-4
2.1.4 no 2-5
2.1.5 service 2-7
2.2 show 2-37
2.2.1 autoinstall 2-42
2.2.2 banner 2-43
2.2.3 commands 2-44

2.2.4 crypto 2-45
2.2.5 environment 2-48
2.2.6 history 2-49
2.2.7 interfaces 2-50
2.2.8 ip 2-52
2.2.9 ldap 2-59
2.2.10 licenses 2-61
2.2.11 logging 2-62
2.2.12 mac 2-63
2.2.13 mac-address-table 2-64
2.2.14 management 2-65
2.2.15 mobility 2-66
2.2.16 ntp 2-69
2.2.17 port-channel 2-71
2.2.18 power 2-72
2.2.19 privilege 2-73
2.2.20 radius 2-74
2.2.21 redundancy dynamic-ap-load-balance 2-75
2.2.22 redundancy -group 2-76
2.2.23 redundancy-history 2-79
2.2.24 redundancy -members 2-80
2.2.25 rtls 2-81
2.2.26 smtp-notification 2-84
2.2.27 snmp 2-86
2.2.28 snmp-server 2-87
2.2.29 spanning-tree 2-90
2.2.30 static-channel-group 2-92
2.2.31 terminal 2-93
2.2.32 timezone 2-94
2.2.33 traffic-shape 2-95
2.2.34 users 2-96
2.2.35 version 2-97
2.2.36 wireless 2-98
2.2.37 wlan-acl 2-112
2.2.38 access-list 2-113
2.2.39 aclstats 2-114
2.2.40 alarm-log 2-115
2.2.41 boot 2-116

2.2.42 clock 2-117
2.2.43 debugging 2-118
2.2.44 dhcp 2-119
2.2.45 file 2-120
2.2.46 ftp 2-121
2.2.47 password-encryption 2-122
2.2.48 running-config 2-123
2.2.49 securitymgr 2-127
2.2.50 sessions 2-128
2.2.51 startup-config 2-129
2.2.52 upgrade-status 2-131
2.2.53 mac-name 2-132
2.2.54 access-list 2-133
2.2.55 aclstats 2-134
2.2.56 alarm-log 2-135
2.2.57 firewall 2-137
2.2.58 role 2-138

Chapter 3. User Exec Commands

3.1 User Exec Commands 3-1
3.1.1 clear 3-3
3.1.2 cluster-cli 3-5
3.1.3 debug 3-6
3.1.4 disable 3-8
3.1.5 enable 3-9
3.1.6 logout 3-10
3.1.7 page 3-11
3.1.8 ping 3-12
3.1.9 quit 3-13
3.1.10 telnet 3-14
3.1.11 terminal 3-15
3.1.12 traceroute 3-16

Chapter 4. Privileged Exec Commands

4.1 Priv Exec Command 4-1
4.1.1 acknowledge 4-4
4.1.2 archive 4-5

4.1.3 cd 4-7
4.1.4 change-passwd. 4-8
4.1.5 clear 4-9
4.1.6 clock 4-13
4.1.7 cluster-cli 4-14
4.1.8 configure 4-15
4.1.9 copy. 4-16
4.1.10 debug 4-17
4.1.11 delete 4-25
4.1.12 diff. 4-26
4.1.13 dir. 4-28
4.1.14 disable 4-29
4.1.15 edit 4-30
4.1.16 enable. 4-31
4.1.17 erase. 4-32
4.1.18 halt 4-33
4.1.19 kill 4-34
4.1.20 logout 4-35
4.1.21 mkdir. 4-36
4.1.22 more 4-37
4.1.23 page 4-39
4.1.24 ping. 4-40
4.1.25 pwd. 4-41
4.1.26 quit 4-42
4.1.27 reload 4-43
4.1.28 rename 4-44
4.1.29 rmdir 4-45
4.1.30 telnet. 4-46
4.1.31 terminal. 4-47
4.1.32 traceroute 4-48
4.1.33 upgrade. 4-49
4.1.34 upgrade - abort 4-51
4.1.35 write 4-52
4.1.36 format 4-54

Chapter 5. Global Configuration Commands

5.1 Global Configuration Commands 5-2

5.1.1 aaa 5-5
5.1.2 access-list 5-7
5.1.3 autoinstall 5-14
5.1.4 banner 5-16
5.1.5 boot 5-17
5.1.6 bridge 5-18
5.1.7 country-code 5-21
5.1.8 crypto 5-22
5.1.8.1 Use Case 1: Configuring Remote VPN 5-33
5.1.8.2 Use Case 2: Configuring Site-to-Site VPN 5-35
5.1.9 do 5-39
5.1.10 end 5-40
5.1.11 errdisable 5-41
5.1.12 ftp 5-42
5.1.13 hostname 5-43
5.1.14 interface 5-44
5.1.15 ip 5-46
5.1.16 license 5-58
5.1.17 line 5-59
5.1.18 local 5-60
5.1.19 logging 5-61
5.1.20 mac 5-64
5.1.21 mac-address-table 5-65
5.1.22 mac-name 5-66
5.1.23 management 5-67
5.1.24 ntp 5-68
5.1.25 prompt 5-73
5.1.26 radius-server 5-74
5.1.27 ratelimit 5-76
5.1.28 redundancy 5-77
5.1.29 role 5-80
5.1.30 rtls 5-82
5.1.31 service 5-83
5.1.32 smtp-notification 5-86
5.1.33 snmp-server 5-94
5.1.34 spanning-tree 5-107
5.1.35 timezone 5-111
5.1.36 traffic-shape 5-112

5.1.37 username 5-115
5.1.37.1 Encrypting a Password 5-116
5.1.38 vpn 5-118
5.1.39 wireless 5-119
5.1.40 wlan-acl 5-120
5.1.41 network-element-id 5-123
5.1.42 firewall 5-124

Chapter 6. Crypto-isakmp Instance

6.1 Crypto ISAKMP Config Commands 6-1
6.1.1 authentication. 6-3
6.1.2 clrscr 6-4
6.1.3 encryption 6-5
6.1.4 end 6-6
6.1.5 exit 6-7
6.1.6 group. 6-8
6.1.7 hash 6-9
6.1.8 help 6-10
6.1.9 lifetime 6-11
6.1.10 no 6-12
6.1.11 service. 6-13
6.1.12 show 6-15

Chapter 7. Crypto-group Instance

7.1 Crypto Group Config Commands 7-1
7.1.1 clrscr 7-3
7.1.2 dns 7-4
7.1.3 end 7-5
7.1.4 exit 7-6
7.1.5 help 7-7
7.1.6 service. 7-8
7.1.7 show 7-9
7.1.8 wins 7-12

Chapter 8. Crypto-peer Instance

8.1 Crypto Peer Config Commands 8-1
8.1.1 clrscr 8-3

8.1.2 end 8-4
8.1.3 exit 8-5
8.1.4 help 8-6
8.1.5 no 8-7
8.1.6 service 8-8
8.1.7 set 8-9
8.1.8 show 8-10

Chapter 9. Crypto-ipsec Instance

9.1 Crypto IPSec Config Commands 9-1
9.1.1 end 9-3
9.1.2 exit 9-4
9.1.3 help 9-5
9.1.4 mode 9-6
9.1.5 no 9-7
9.1.6 show 9-8
9.1.7 service 9-10

Chapter 10. Crypto-map Instance

10.1 Crypto Map Config Commands 10-1
10.1.1 clrscr 10-3
10.1.2 end 10-4
10.1.3 exit 10-5
10.1.4 help 10-6
10.1.5 match 10-7
10.1.6 no 10-9
10.1.7 service 10-10
10.1.8 set 10-12
10.1.9 show 10-16

Chapter 11. Crypto-trustpoint Instance

11.1 Trustpoint (PKI) Config Commands 11-1
11.1.1 clrscr 11-3
11.1.2 company-name 11-4
11.1.3 email 11-5
11.1.4 end 11-6
11.1.5 exit 11-7

11.1.6 fqdn 11-8
11.1.7 help 11-9
11.1.8 ip-address 11-10
11.1.9 no 11-11
11.1.10 password 11-12
11.1.11 rsakeypair 11-13
11.1.12 service 11-14
11.1.13 show 11-15
11.1.14 subject-name 11-17

Chapter 12. Interface Instance

12.1 Interface Config Commands 12-1
12.1.1 clrscr 12-3
12.1.2 crypto 12-4
12.1.3 description 12-5
12.1.4 duplex 12-6
12.1.5 end 12-7
12.1.6 exit 12-8
12.1.7 help 12-9
12.1.8 ip 12-10
12.1.8.1 Creating Helper Address using DHCP Server 12-12
12.1.8.2 Configuring a Static NAT Source Translation 12-12
12.1.9 mac 12-13
12.1.10 management 12-14
12.1.11 no 12-15
12.1.12 port-channel 12-16
12.1.12.1 Configuring a Port Aggregation 12-17
12.1.13 power 12-19
12.1.14 service 12-21
12.1.15 show 12-22
12.1.16 shutdown 12-24
12.1.17 spanning-tree 12-25
12.1.18 speed 12-28
12.1.19 static-channel-group 12-29
12.1.20 switchport 12-30
12.1.21 storm-control 12-32

Chapter 13. Spanning tree-mst Instance

13.1 mst Config Commands 13-1
13.1.1 clrscr 13-3
13.1.2 end 13-4
13.1.3 exit 13-5
13.1.4 help 13-6
13.1.5 instance 13-7
13.1.6 name 13-8
13.1.7 no 13-9
13.1.8 revision 13-10
13.1.9 service 13-11
13.1.10 show 13-13

Chapter 14. Extended ACL Instance

14.1 Extended ACL Config Commands 14-1
14.1.1 clrscr 14-3
14.1.2 deny 14-4
14.1.2.1 Example - Denying Traffic Between Two Subnets 14-8
14.1.2.2 Example - Denying TCP Based Traffic 14-8
14.1.2.3 Example - Denying UDP Based Traffic 14-9
14.1.2.4 Example - Denying ICMP Based Traffic 14-9
14.1.3 end 14-10
14.1.4 exit 14-11
14.1.5 help 14-12
14.1.6 mark 14-13
14.1.6.1 Example - Marking dot1p on TCP Based Traffic 14-17
14.1.6.2 Example - Marking tos on TCP based Traffic 14-17
14.1.7 no 14-19
14.1.8 permit 14-20
14.1.8.1 Permitting IP Based Traffic 14-24
14.1.8.2 Permitting Telnet Based Traffic 14-24
14.1.8.3 Permitting ICMP Based Traffic 14-24
14.1.9 service 14-25
14.1.10 show 14-26
14.2 Configuring IP Extended ACL 14-28

Chapter 15. Standard ACL Instance

15.1 Standard ACL Config Commands 15-1
15.1.1 clrscr 15-3
15.1.2 deny 15-4
15.1.2.1 Example - Denying Traffic to the Interface 15-5
15.1.2.2 Example - Denying Traffic only from Source Network 15-5
15.1.3 end 15-6
15.1.4 exit 15-7
15.1.5 help 15-8
15.1.6 mark 15-9
15.1.6.1 Marking tos for Source Network Traffic 15-10
15.1.7 no 15-11
15.1.8 permit 15-12
15.1.8.1 Example - Permitting Traffic to Interface 15-13
15.1.8.2 Permitting Traffic from Source Network 15-13
15.1.9 service 15-14
15.1.10 show 15-16
15.2 Use Case: Configuring IP Standard ACL 15-18

Chapter 16. Extended MAC ACL Instance

16.1 MAC Extended ACL Config Commands 16-1
16.1.1 clrscr 16-3
16.1.2 deny 16-4
16.1.2.1 Example - Denying Traffic from any MAC Address 16-6
16.1.2.2 Example - Denying dot1q Tagged Traffic 16-6
16.1.2.3 Example - Denying Traffic Between Two MAC Based Hosts 16-6
16.1.3 end 16-7
16.1.4 exit 16-8
16.1.5 help 16-9
16.1.6 mark 16-10
16.1.6.1 Example - Marking dot1p Priority Value for 802.1q Tagged Traffic 16-12
16.1.6.2 Example - Marking tos for IP Traffic 16-12
16.1.7 no 16-13
16.1.8 permit 16-14
16.1.8.1 Example - Permitting WISP Traffic 16-16
16.1.8.2 Example - Permitting ARP Traffic 16-16

16.1.8.3 Permitting IP Traffic 16-17
16.1.9 service 16-18
16.1.10 show 16-20
16.2 Configuring MAC Extended ACL 16-23

Chapter 17. DHCP Server Instance

17.1 DHCP Config Commands 17-1
17.1.1 address 17-4
17.1.2 bootfile 17-5
17.1.3 class 17-6
17.1.3.1 Creating a DHCP User Class 17-6
17.1.3.2 config-dhcp-class 17-7
17.1.4 client-identifier 17-9
17.1.5 client-name 17-10
17.1.6 clrscr 17-11
17.1.7 ddns 17-12
17.1.8 default-router 17-14
17.1.9 dns-server 17-15
17.1.10 domain-name 17-16
17.1.11 end 17-17
17.1.12 exit 17-18
17.1.13 hardware-address 17-19
17.1.14 help 17-20
17.1.15 host 17-21
17.1.16 lease 17-22
17.1.17 netbios-name-server 17-24
17.1.18 netbios-node-type 17-25
17.1.19 network 17-26
17.1.20 next-server 17-27
17.1.21 no 17-28
17.1.22 option 17-29
17.1.23 service 17-30
17.1.24 show 17-31
17.1.25 update 17-33
17.1.26 unitcast-enable 17-34
17.2 Configuring the DHCP Server using Switch CLI 17-35
17.2.1 Creating network pool 17-36

17.2.2 Creating a Host Pool 17-37
17.2.3 Troubleshooting DHCP Configuration 17-38
17.2.4 Creating a DHCP Option 17-40

Chapter 18. DHCP Class Instance

18.1 DHCP Server Class Config Commands 18-1
18.1.1 clrscr 18-3
18.1.2 end 18-4
18.1.3 exit 18-5
18.1.4 help 18-6
18.1.5 multiple-user-class 18-7
18.1.6 no 18-8
18.1.7 option 18-9
18.1.7.1 Creating a DHCP User Class 18-9
18.1.8 service 18-11
18.1.9 show 18-12

Chapter 19. Radius Server Instance

19.1 Radius Configuration Commands 19-1
19.1.1 authentication 19-3
19.1.2 ca 19-5
19.1.3 clrscr 19-6
19.1.4 crl-check 19-7
19.1.5 end 19-8
19.1.6 exit 19-9
19.1.7 group 19-10
19.1.7.1 clrscr 19-11
19.1.7.2 end 19-11
19.1.7.3 exit 19-11
19.1.7.4 group 19-12
19.1.7.5 guest-group 19-12
19.1.7.6 help 19-13
19.1.7.7 no 19-14
19.1.7.8 policy 19-15
19.1.7.9 rad-user 19-17
19.1.7.10 rate-limit 19-17

19.1.7.11 service 19-18
19.1.7.12 show 19-19
19.1.7.13 Example–Creating a Group 19-20
19.1.8 help 19-23
19.1.9 ldap-server 19-24
19.1.10 nas 19-27
19.1.11 no 19-28
19.1.12 proxy 19-29
19.1.13 rad-user 19-31
19.1.14 server 19-34
19.1.15 service 19-35
19.1.16 show 19-36
19.1.17 ldap-group-verification 19-38

Chapter 20. Wireless Instance

20.1 Wireless Configuration Commands 20-1
20.1.1 aap 20-5
20.1.2 admission-control 20-7
20.1.3 adopt-unconf-radio 20-8
20.1.4 adoption-pref-id 20-9
20.1.5 ap 20-10
20.1.6 ap-containment 20-13
20.1.7 ap-detection 20-14
20.1.8 ap-image 20-16
20.1.9 ap-ip 20-17
20.1.10 ap-standby-attempts-threshold 20-19
20.1.11 ap-timeout 20-20
20.1.12 ap-udp-port 20-21
20.1.13 auto-select-channels 20-22
20.1.14 broadcast-tx-speed 20-23
20.1.15 client 20-24
20.1.15.1 Configuring a Client 20-25
20.1.15.2 config-wireless-client-list Commands 20-26
20.1.16 clrscr 20-28
20.1.17 cluster-master-support 20-29
20.1.18 convert-ap 20-30
20.1.18.1 Converting an AP to Sensor 20-32

20.1.19 country-code 20-33
20.1.20 debug 20-34
20.1.21 dhcp-one-portal-forward 20-37
20.1.22 dhcp-sniff-state 20-38
20.1.23 dot11-shared-key-auth 20-39
20.1.24 end 20-40
20.1.25 exit 20-41
20.1.26 fix-broadcast-dhcp-rsp 20-42
20.1.27 help 20-43
20.1.28 hotspot 20-44
20.1.29 ids 20-45
20.1.30 load-balance 20-50
20.1.31 mac-auth-local 20-51
20.1.32 manual-wlan-mapping 20-53
20.1.33 mobile-unit 20-54
20.1.34 mobility 20-55
20.1.35 multicast-packet-limit 20-56
20.1.36 multicast-throttle-watermark 20-57
20.1.37 nas-id 20-58
20.1.38 nas-port-id 20-59
20.1.39 no 20-60
20.1.40 proxy-arp 20-61
20.1.41 qos-mapping 20-62
20.1.42 radio 20-64
20.1.43 rate-limit 20-78
20.1.44 secure-wispe-default-secret 20-79
20.1.45 self-heal 20-80
20.1.46 sensor 20-82
20.1.47 service 20-84
20.1.48 show 20-97
20.1.49 smart-rf 20-100
20.1.50 smart-scan-channels 20-101
20.1.51 wlan 20-102
20.1.52 wlan-bw-allocation 20-127

Chapter 21. RTLS Instance

21.1 RTLS Config Commands 21-1

21.1.1 aeroscout 21-3
21.1.2 clear 21-4
21.1.3 clrscr 21-5
21.1.4 end 21-6
21.1.5 espi 21-7
21.1.6 exit 21-8
21.1.7 help 21-9
21.1.8 ekahau 21-10
21.1.9 no 21-11
21.1.10 reference-tag 21-14
21.1.11 rfid 21-16
21.1.12 service 21-17
21.1.13 show 21-20
21.1.14 site 21-23
21.1.15 sole 21-25
21.1.16 switch 21-26
21.1.17 zone 21-27
21.1.18 ap 21-28

Chapter 22. ESPI Instance

22.1 ESPI Config Commands 22-1
22.1.1 adapter 22-3
22.1.2 clrscr 22-4
22.1.3 end 22-5
22.1.4 exit 22-6
22.1.5 help 22-7
22.1.6 no 22-8
22.1.7 service 22-9
22.1.8 show 22-10

Chapter 23. RFID Instance

23.1 RFID Config Commands 23-1
23.1.1 activate 23-3
23.1.2 clrscr 23-4
23.1.3 end 23-5
23.1.4 exit 23-6
23.1.5 help 23-7

23.1.6 no 23-8
23.1.7 reader 23-9
23.1.8 service 23-12
23.1.9 show 23-15

Chapter 24. SOLE Instance

24.1 SOLE Config Commands 24-1
24.1.1 clrscr 24-3
24.1.2 end 24-4
24.1.3 exit 24-5
24.1.4 help 24-6
24.1.5 locate 24-7
24.1.6 no 24-9
24.1.7 redundancy 24-10
24.1.8 service 24-11
24.1.9 show 24-12
24.1.10 rssi-filter 24-15
24.1.11 aap-rssi-update-interval 24-16
24.1.12 mobile-unit 24-17

Chapter 25. Smart RF Instance

25.1 smart-rf Config Commands 25-1
25.1.1 assignable-power-range 25-3
25.1.2 auto-assign 25-4
25.1.3 clrscr 25-5
25.1.4 end 25-6
25.1.5 exit 25-7
25.1.6 extensive-scan 25-8
25.1.7 help 25-9
25.1.8 hold-time 25-10
25.1.9 no 25-11
25.1.10 number-of-rescuers 25-18
25.1.11 radio 25-19
25.1.12 recover 25-23
25.1.13 retry-threshold 25-24
25.1.14 run-calibrate 25-25
25.1.15 scan-dwell-time 25-26

25.1.16 schedule-calibrate 25-27
25.1.17 select-channels. 25-28
25.1.18 service. 25-29
25.1.19 show 25-33
25.1.20 smart-rf-module 25-39
25.1.21 verbose 25-40

Chapter 26. Role Instance

26.1 Role Config Commands 26-1
26.1.1 ap-location 26-3
26.1.2 authentication-type 26-5
26.1.3 encryption-type. 26-6
26.1.4 essid 26-8
26.1.5 group. 26-9
26.1.6 ip 26-10
26.1.7 mac 26-11
26.1.8 mu-mac 26-12
26.1.9 clrscr 26-13
26.1.10 no 26-14
26.1.11 end 26-15
26.1.12 exit 26-16
26.1.13 help 26-17
26.1.14 service. 26-18
26.1.15 show 26-19

1

Introduction

This chapter describes the commands defined by the switch *Command Line Interface* (CLI). Access the CLI (on the supported RFS6000 and RFS7000 models) by running a terminal emulation program on a computer connected to the serial port on the front of the switch, or by using a Telnet session via *secure shell* (SSH) to access the switch over the network. The default CLI user designation is **cli**. The default username and password are *admin* and *superuser* respectively.

To avoid confusion amongst RFS6000 and RFS7000 CLI users, generic examples are used throughout this guide. These examples are relevant to each switch.

Example

```
RFSwitch>cluster-cli enable
RFSwitch>
```

The CLI syntax, parameters and descriptions within this guide can also be used generically for a RFS6000 and RFS7000 model switch. However, some subtle differences do exist amongst these baselines. These differences are noted within the specific commands impacted. When these differences are noted, the options available to each switch baseline are described in detail.

1.1 CLI Overview

The CLI is used for configuring, monitoring, and maintaining the switch managed network. The user interface allows you to execute commands (on the supported RFS6000 and RFS7000 models) using either a serial console or a remote access method.

This chapter describes the basic features of the CLI. Topics covered include an introduction to command modes, navigation and editing features, help features, and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular RFS6000 or RFS7000 model used. Enter a question mark (**?**) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the configuration of the switch (such as determining the current switch configuration).

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

Most of the USER EXEC mode commands are one-time commands and are not saved across switch reboots. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across switch reboots.

Access a variety of protocol-specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you access specific configuration modes only through the global configuration mode.

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

Table 1.1 summarizes the commands available from the switch.

Table 1.1 RF Switch CLI Hierarchy

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
clear	acknowledge	aaa
clrscr	archive	access-list
cluster-cli	cd	autoinstall
debug	change-passwd	banner
disable	clear	boot
enable	clock	bridge
exit	clrscr	clrscr
help	cluster-cli	country-code
logout	configure	crypto
no	copy	do
page	debug	end
ping	delete	errdisable
quit	diff	exit
service	dir	fallback
show	disable	format
telnet	edit	ftp
terminal	enable	help
traceroute	erase	hostname
	exit	interface
	halt	ip
	help	license

Table 1.1 RF Switch CLI Hierarchy

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
	kill	line
	logout	local
	mkdir	logging
	more	mac
	no	mac-address-table
	page	mac-name
	ping	management
	pwd	no
	quit	ntp
	reload	prompt
	rename	radius-server
	rmdir	redundancy
	service	rtls
	show	service
	telnet	show
	terminal	smtp-notification
	traceroute	snmp-server
	upgrade	spanning-tree
	upgrade-abort	timezone
	write	traffic-shape
	format	username

Table 1.1 RF Switch CLI Hierarchy

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
		vpn
		wireless
		wireless-acl
		firewall
		network-element-id
		ratelimit
		role

1.2 Getting Context Sensitive Help

Enter a question mark (**?**) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	***Description***
(prompt)# help	Displays a brief description of the help system
*(prompt)# abbreviated-command-entry***?**	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# **?**	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command

Command	***Description***
(prompt)# command keyword ?	Lists the next available syntax option for the command



NOTE: The system prompt varies depending on which configuration mode you are in.



NOTE: Enter **Ctrl + V** to use **?** as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?



NOTE: The escape character used through out the CLI is "\". To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word.

```
RFSwitch#service?
  service Service Commands

RFSwitch#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the **?**. This form of help is called **command syntax help.** It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
RFSwitch>service ?
  diag      Diagnostics
  encrypt   Encrypt password or key with secret
  save-cli  Save CLI tree for all modes in html format
  show      Show running system information

RFSwitch>service
```

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as `config t`. Since the abbreviated command is unique, the switch accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
RFSwitch>help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch>
```

1.3 Using the No and Default Command Forms

Almost every command has a no form. Use no to disable a feature or function. Use the command without the no keyword to re-enable a disabled feature or enable a feature disabled by default.

1.3.1 Basic Conventions

Keep the following conventions in mind while working within the CLI:

- Use **?** at the end of a command to display available sub-modes . Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using **?** until you reach the last sub-mode
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`

- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive
- If an instance name (or other parameter) contains whitespace, the name must be enclosed in quotes

```
RFSwitch.(Cfg)> spol "Default Switch Policy"
RFSwitch.(Cfg).SPolicy.[Default Switch Policy]>
```



NOTE: Commands starting with `#` at the `RFSwitch#` prompt are ignored and not executed. Any space before a CLI command is ignored in execution.

1.4 Using CLI Editing Features and Shortcuts

A variety of shortcuts and edit features are available. The following describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Deleting Entries*
- *Re-displaying the Current Command Line*
- *Transposing Mistyped Characters*
- *Controlling Capitalization*

1.4.1 Moving the Cursor on the Command Line

Table 1.2 shows the key combinations or sequences to move the cursor on the command line. **Ctrl** defines the Control key, which must be pressed simultaneously with its associated letter key.

Esc supports the Escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. In Table 1.2, bold characters bold indicate the relation between a letter and its function.

Table 1.2 Key Combinations Used to Move the Cursor

Keystrokes	***Function Summary***	***Function Details***
Left Arrow *or* ***Ctrl-B***	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to scroll back to the system prompt and verify the beginning of the command entry. You can press the Ctrl-A key combination.
Right Arrow *or* ***Ctrl-F***	Forward character	Moves the cursor one character to the right
Esc, B	Back word	Moves the cursor back one word
Esc, F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-d		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the rest of a word to uppercase
Esc-L		Converts the rest of a word to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor

Keystrokes	***Function Summary***	***Function Details***
Ctrl-Z		Enters the command and returns to the root prompt
Ctrl-L		Refreshes the input line

1.4.2 Completing a Partial Command Name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform) enter the first few letters of a command, then press the **Tab** key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-I.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter "conf" within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with `conf`.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
RFSwitch# conf<Tab>
RFSwitch# configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the **Return** or **Enter** key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering `co?` lists all commands available in the current command mode:

```
RFSwitch# co?
copy? commit
```

```
RFSwitch# co
```

NOTE: The characters entered before the question mark are reprinted to the screen to complete the command entry.

1.4.3 Deleting Entries

Use any of the following keys (or key combinations) to delete command entries:

Keystrokes	*Purpose*
Backspace	Deletes the character to the left of the cursor
Ctrl-D	Deletes the character at the cursor
Ctrl-K	Deletes all characters from the cursor to the end of the command line
Ctrl-W	Deletes a word up to the cursor
Esc, D	Deletes from the cursor to the end of the word

1.4.4 Re-displaying the Current Command Line

If entering a command and the system suddenly sends a message, you can recall the current command entry. To re-display the current command line (refresh the screen), use the following key combination:

Keystrokes	*Purpose*
Ctrl-L	Re-displays the current command line

1.4.5 Command Output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a `Press Any Key to Continue (Q to Quit)` prompt displays at the bottom of the screen. To resume the output, press the Return key to scroll down one line or press the Spacebar to display the next full screen of output.

1.4.6 Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters. To transpose characters, use the following key combination:

Keystrokes	Purpose
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor

1.4.7 Controlling Capitalization

Capitalize or lowercase words with a few simple key sequences. The switch CLI commands are generally case-insensitive (and in lowercase). To change the capitalization of the commands, use one of the following sequences:

Keystrokes	Purpose
Esc, C	Capitalizes the letters to the right of cursor
Esc, L	Changes the letters at the right of cursor to lowercase

2

Common Commands

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains those commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

2.1 Common Commands

Table 2.1 summarizes available common commands:

Table 2.1 Common Commands in RFSwitch

Command	Description	Ref.
clrscr	Clears the display screen	*page 2-2*
exit	Ends the current mode and moves to the previous mode	*page 2-3*
help	Displays the interactive help system	*page 2-4*
no	Negates a command or sets its defaults	*page 2-5*
service	Services or debugs the switch	*page 2-7*
show	Shows running system information	*page 2-37*

2.1.1 clrscr

Common Commands

Clears the screen and refreshes the prompt (**#**)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch#clrscr
RFSwitch#
```

2.1.2 exit

Common Commands

Ends the current mode and moves to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config)#exit
RFSwitch#
```

2.1.3 help

Common Commands

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic.

Two kinds of help are provided:

1. Full help is available when ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

or

?

Parameters

None

Example

```
RFSwitch>
diag      Diagnostics
encrypt   Encrypt password or key with secret
kill      Kill a connection
locator   flash all LEDS to locate switch visually
save-cli  Save CLI tree for all modes in html format
show      Show running system information
undefine  Undefine non active Event Cycle spec
wireless  Wireless parameters
RFSwitch>
```

2.1.4 no

Common Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

no

Parameters

None

Example (User Exec)

```
RFSwitch>no ?
 cluster-cli Cluster context
 debug    Debugging functions
 page     Toggle paging
 service   Service Commands
RFSwitch>no
```

Example (Priv Exec)

```
RFSwitch#no ?
 cluster-cli Cluster context
 debug    Debugging functions
  mobile-unit  mobile-unit index
 page     Toggle paging
 service   Service Commands
 upgrade   Name of the patch to remove
RFSwitch#no
```

Example (Global Config)

```
RFSwitch(config)#no ?
 aaa        VPN AAA authentication settings
 access-list    Configure access-lists
 autoinstall    autoinstall configuration command
 banner       Reset login banner to nothing
 bridge       Bridge group commands
```

```
 country-code    Clear the currently configured country
code. All existing configurations will be erased
 crypto       encryption module
 errdisable     errdisable
  firewall          Wireless firewall
 fallback      Configures software fallback feature
 ftp        Configure FTP Server
 hostname      Reset system's network name to default
 interface     Delete a virtual interface
 ip         Internet Protocol (IP)
 line        Configure a terminal line
 local       Local user authentication database for VPN
 logging      Modify message logging facilities
 mac        MAC configuration
 mac-address-table Configure MAC address table
  mac-name          Remove a configured MAC Address name
 management     sets properties of the management interface
  network-element-id Reset system’s network element
 ntp        Configure NTP
 prompt       Reset system's prompt
 radius-server   RADIUS server configuration commands
  ratelimit         ratelimit
  role              Configure role parameters
 redundancy     Configure redundancy group parameters
 service      Service Commands
 smtp-notification Modify SMTP-Notification parameters
 snmp-server    Modify SNMP engine parameters
 spanning-tree   Spanning tree
 timezone      Revert the timezone to default (UTC)
 traffic-shape   Traffic shaping
 username      Establish User Name Authentication
 vpn        vpn
 wlan-acl      Remove an ACL from WLAN

RFSwitch(config)#no
```

2.1.5 service

Common Commands

Service commands are used to manage the switch configuration in all modes. Depending on the mode, different service commands will display.

- RFS7000
- RFS6000

Syntax (User Executable Mode)

```
service [diag|encrypt|kill|locator|save-cli|show|undefine|
  wireless]
service [locator|save-cli|undefine]

service diag [enable|identify|limit|period|
  tech-support-period|tech-support-url]
service diag [enable|identify]
service diag limit [buffer|fan|filesys|inodes|load|maxFDs|
  pkbuffers|procRAM|ram|routecache|temperature]
service diag limit buffer
  [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k]
service diag limit fan <1-3> low <1000-15000>
service diag limit filesys [etc2|flash|var]
  <limit-as-percent>
service diag limit inodes [etc2|flash|var]
  <limit-as-percent>
service diag limit load [01|05|15] <load-as-percent>
service diag limit maxFDs <0-32767>
service diag limit pkbuffers <0-65535>
service diag limit procRAM <0.0-100.0>
service diag limit ram <0.0-25.0>
service diag limit routecache <0-65535>
service diag limit temperature <temp-sensor-number>
[critical|high|low] <temperature>
service diag period <100-30000>
service diag tech-support-period <10-10080>
service diag tech-support-url <URL>

service encrypt secret 2 <passphrase> plaintext <plaintext>
service kill connection {<1-64>}

service show [cli|command-history|crash-info|diag|info|
  memory|process|reboot-history|rtls|startup-log|
  upgrade-history|watchdog]
```

service show [cli|command-history|crash-info|info|memory|
process|reboot-history|startup-log|upgrade-history|
watchdog]

service show diag [hardware|led-status|limits|period|stats|
tech-support-period|tech-support-url|top]

service show rtls [location-history|rfid]
service show rtls location-history
service show rtls rfid events reader *{<1-48>}*

service undefine ecspec *{<ECSpec-name>}*

service wireless

Parameters (User Executable Mode)

diag [enable|identify|limit| period| tech-support-period| tech-support-url]	Diagnostics commands • enable – Enables in-service diagnostics • identify – Identifies a switch by flashing its LEDs • limit [buffer|fan|filesys|inodes|load|maxFDs| pkbuffers|procRAM|ram|routecache|temperature] – Sets the diagnostic limit command • buffer []<0-65535> – Configures the buffer usage warning limit. The warning limit can be set to a buffer limit size [128|128k|16k|1k|256|2k|32|32k|4k| 512|64|64k|8k]. • <0-65535>– Configures buffer usage warning limit. Set between 0 and 65535. • fan <1 -3> low <1000-15000> – Sets the fan speed limit for the fans on the switch. • low <1000-15000> – Sets the low speed limit of the selected fan in RPMs. • filesys [etc2|flash|var] – Sets the file system freespace limit • inodes[etc2|flash|var] – File system inode limit • load [01|05|15] – Aggregate processor load • maxFDs <0-32767> – Configures the maximum number of file descriptors. Set between 0 to 32767 • pkbuffers <0-65535> – Configures the packet buffer head cache limit. Set between 0 and 65535. • procRAM <0-100.0> – Defines the RAM space used by a process. Set the percentage <percent> of RAM space used by the processor between 0.0 and 100.0 percent. • ram <0.0-25.0> – Configures free space for the RAM. Configures the free space to any value between 0.0 to 25.0 percent.

	• routecache <0-65535> – Configures IP route cache usage. Set a value between 0 and 65553. • temperature <1-6> [critical|high|low] – Sets the number of temperature sensors for the switch. • critical <0.0 - 250.0> – Critical temperature limit • high <0.0 - 250.0> – high temperature limit • low <0.0 - 250.0> – low temperature limit • period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milliseconds. The default value is 1000 milliseconds. • tech-support-period <10-10080> – Sets diagnostics tech-support-period • <10-10080> – The default 1440 minutes (1 day) • tech-support-url <URL>– Set the URL to use during auto generated technical support dumps • <URL> – URL to which to copy • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>@<hostname|IP>[:port]>/path/file
encrypt secret 2 <pass-phrase> plaintext <plain-text>	Encrypts a password or key with a secret passphrase • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Defines the passphrase used for encryption • <plain-text> – Defines the plain text password or key to encrypt
kill connection *{<1-64>}*	Kills a connection using ESPI Adapter index • connection *{<1-64>}* – A single optional ESPI Adapter index <1-64>
locator	Locates the switch by flashing all LEDs.

save-cli	Saves the CLI tree for all modes in HTML
show [cli|command-history|crash-info|diag|info|memory|process|reboot-history|rtls|startup-log|upgrade-history|watchdog]	Displays running system information • cli – Shows the CLI tree of the current mode • command-history – Displays the command (except show commands) history • crash-info – Displays information about core, panic and AP dump files • diag [hardware|led-status|limits|period|stats|tech-support-period|tech-support-url|top] – Sets or displays switch diagnostics • hardware – Shows the system hardware configuration • led-status – Shows LED state variables and the current state • limits – Shows limit values • period – Shows the period (ms) for in-service diagnostics • stats – Shows current diagnostics statistics • top – Shows the top processes (sorted by memory usage) • tech-support-period <10-10080> – Shows diagnostics tech-support-period • <10-10080> – The default 1440 minutes (1 day) • tech-support-url <URL> –Shows the URL to use during auto generated technical support dumps • <URL> – URL to which to copy • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>@<hostname|IP>[:port]>/path/file

	• info – Shows a snapshot of available support information • memory – Shows memory statistics • watchdog – Shows watchdog status • process – Shows processes (sorted by memory usage) • reboot-history – Shows a reboot history • startup-log – Shows the startup log • upgrade-history – Shows an upgrade history • rtls [location-history|rfid] – Real Time Locationing System commands • location-history – Show location engine history • rfid events – RFID Configuration • events reader – RFID reader events • reader <1-48> – A single RFID reader index • watchdog – Shows watch dog status
undefine ecspec *{<SPECNAME>}*	Undefines non active Event Cycle Specification • ecspec *{<SPECNAME>}* – Name of optional ECSpecs configuration
wireless	Displays current wireless parameters

Syntax (Privilege Executable Mode) (Priv Exec)

```
service [clear|copy|dhcp-snoop-conflict-detection|diag|
  diag-shell|encrypt|firewall|kill|locator|pktcap|pm|
  save-cli|securitymgr|show|smart-rf|start-shell|undefine|
  watchdog|wireless]
service [diag-shell|locator|pm stop|save-cli|start-shell|
  watchdog]

service clear [all|aplogs|clitree|cores|dumps|fw|panics|
  snooptable|wireless]
service clear securitymgr flows [<flow-index>|<interface>|
  all|ge <ge-index>|me1|sa <sa-index>|vlan <vlan-id>]

service copy tech-support [<file>|<URL>] [tftp|ftp|sftp]

service dhcp-snoop-conflict-detection disable
```

service diag [enable|identify|limit|period|
tech-support-period|tech-support-url]

service encrypt secret 2 <pass-phrase> <plain-text>
service firewall disable
service kill conncection *{<1-64>}*

service pktcap on [bridge|deny|drop|interface|router|vlan]
service pktcap on [bridge|drop] *{[count <1-99999>|filter|hex|snap|verbose|write]}*
service pktcap on bridge filter on
[<LINE>|arp|capwap|dst|ether|host|icmp|igmp|ip|ip6|l2|l3|
l4|net|not|port|src|tcp|udp|vlan|wlan]
service pktcap on bridge **filter** [arp|capwap|icmp|ip|ip6|
igmp|udp] *{[and|or]*
<LINE>}
service pktcap on bridge filter capwap *{[ctrl|data] [and|or]*
<LINE>}
service pktcap on bridge filter dst [A.B.C.D|net|port]
{[and|or] <LINE>}
service pktcap on bridge filter ether [broadcast|dst|host|
multicast|proto|src]
service pktcap on bridge filter ether [broadcast|multicast]
{[and|or] <LINE>}
service pktcap on bridge filter ether [dst|host|src] <MAC>
{[and|or] <LINE>}
service pktcap on bridge filter ether proto <0-65535>
{[and|or] <LINE>}
service pktcap on bridge filter ether host <IP> *{[and|or]*
<LINE>}
service pktcap on bridge filter ip multicast *{[and|or]*
<LINE>}
service pktcap on bridge filter ip proto [<0-255>|
<protocol>] *{[and|or] <LINE>}*
service pktcap on bridge filter [l2|l3|l4] [u16 <0-126>|
u32 <0-124>|u8 <0-127>]
service pktcap on bridge filter net <IP/MASK> *{[and|or]*
<LINE>}
service pktcap on bridge filter not [arp|capwap|dst|ether|
host|icmp|igmp|ip|ip6|l2|l3|l4|net|not|port|src|tcp|udp|
vlan|wlan]
service pktcap on bridge filter port <0-65535> *{[and|or]*
<LINE>}
service pktcap on bridge filter src [<IP>|net <IP/MASK>|
port <0-65536>] *{[and|or] <LINE>}*

```
service pktcap on bridge filter tcp {[[and|or]
<LINE>|[ack|fin|or|rst|syn] {[and|or] <LINE>]}
service pktcap on bridge filter vlan <1-4095> {[and|or]
<LINE>}
service pktcap on bridge filter wlan <1-2> {[and|or] <LINE>}
service pktcap on bridge [hex|verbose] {[count <1-1000000>|
  filter [...] |snap <1-1518>]}
service pktcap on bridge snap <1-1518> {filter [...]}
service pktcap on bridge write [<FILE>|<URL>]
  {[count <1-1000000>|filter [...] |snap <1-1518>]}
service pktcap on deny [access-list|count|filter|
  hex|inbound|outbound|snap|verbose|write]
service pktcap on deny access-list <ACL-index> {[and|or]
  <LINE>}
service pktcap on deny [inbound|outbound] {[access-list|
  count|filter|hex|[inbound|outbound]|snap|verbose|write]}
  {[and|or] <LINE>}
service pktcap on interface [<INTERFACE>|ge <1-4>|me1|
  sa <1-4>|vlan <1-4094>] {[count|filter|hex|inbound|
  outbound|snap|verbose|write]} {[and|or] <LINE>}
service pktcap on router {[count|filter|hex|snap|verbose|
  write]} {[and|or] <LINE>}
service pktcap on vpn {[count|filter|hex|inbound|outbound|
  snap|verbose|write]} {[and|or] <LINE>}

service securitymgr [disable|disable-flow-rate-limit|
  dump-core|enable-http-stats]

service show [cli|command-history|crash-info|diag|fw|info|
ip|last-passwd|memory|pm|process|reboot-history|rtls|
securitymgr|smart-rf|startup-log|upgrade-history|watchdog|
wireless]
service show [cli|command-history|crash-info|diag|info|
  memory|process|reboot-history|rtls|startup-log|
  upgrade-history|watchdog]

service show fw flows brief
service show ip igmp snooping vlan <1-4094> {<MULTICAST-IP>}
service show last-passwd
service show pm {history [<process-name>|all]

service show rtls [grid|location-history|rfid]
service show rtls grid [all|x]
service show rtls grid all
service show rtls grid x <0-9000> y <0-9000>
service show rtls rfid events reader {<1-48>}
```

```
service show securitymgr flows [details|source]
service show securitymgr flows details {source [<IP>|any]
  destination [<IP>|any] protocol [any|icmp|tcp|udp]}
service show securitymgr flows source [<IP>|any] destination
[<IP>|any] protocol [any|icmp|tcp|udp]

service show smart-rf [debug-config|sensitivity]
service show smart-rf debug-config
service show smart-rf sensitivity [mu|pattern|rates]
service show smart-rf sensitivity mu {<1-8192>|<MAC>}
service show smart-rf sensitivity pattern [pattern-
11a|pattern-11b|pattern-11bg|pattern-2-mbps]

service show wireless [ap-history|buffer-counters|
  enhanced-beacon-table|enhanced-probe-table|group|
  group-stats|legacy-load-balance|mu-cache-buckets|
  mu-cache-entry|mvlan|radio|radio-cache-entry|
  radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|
  vlan-cache-entry|waiting]
service show wireless [buffer-counters|group-stats|
  legacy-load-balance|mu-cache-buckets|radio-hash-buckets|
  snmp-trap-throttle|vlan-cache-buckets]

service show wireless ap-history <MAC>
service show wireless[enhanced-beacon-table|
  enhance-probe-table] [config|report]
service show wireless group <1-256>
service show wireless mu-cache-entry {<1-8192>|<MAC>}
service show wireless mvlan <1-256>
service show wireless radio [<1-4096>|description|mapping]
service show wireless radio-cache-entry {<MAC>}
service show wireless vlan-cache-entry {[<1-8192>|<MAC>]}
service show wireless waiting {<1-99>}

service smart-rf [clear-history|load-from-
file|replay|rescue|restore|save-to-file|simulate]
service smart-rf replay enable
service smart-rf [rescue|restore] [<radio-mac>|
  <radio-index>|<radio-index-list>]
service smart-rf simulate [coverage-hole|interference]
service smart-rf simulate coverage-hole <1-4096>
  <unit-range> [<unit-range>|pattern-11a|pattern-11b|
  pattern-11bg|pattern-2-mbps]
service smart-rf interference [<radio-mac>|<radio-index>|
  <radio-index-list>]
```

```
service undefine ecspec {<SPECNAME>}

service wireless [ap-history|clear-ap-log|custom-cli|dot11i|
  dump-core|enhanced-beacon-table|enhanced-probe-table|
  free-packet-watermark|idle-radio-send-multicast|
  legacy-load-balance|map-radios|radio-misc-cfg|rate-scale|
  request-ap-log|save-ap-log|snmp-trap-throttle|
  sync-radio-entries|vlan-cache]
service wireless [dumpcore|legacy-load-balance|rate-scale|
  save-ap-log|sync-radio-entries]
service wireless ap-history [clear|enable]
service wireless clear-ap-log {<1-1024>}

service wireless custom-cli [sh-wi-mobile-unit|sh-wi-radio]
service wireless custom-cli sh-wi-mobile-unit [ap-locn|
  ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|
  radio-desc|radio-id|ssid|state|vlan|wlan-desc|wlan-id|
  username]
service wireless custom-cli sh-wi-radio [adopt-info|
  ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-mu|
  power|radio-desc|radio-id|state]

service wireless dot11i enforce pmkid-validation

service wireless enhanced-beacon-table [channel-set|enable|
  erase-report|max-ap|scan-interval|scan-time]
service wireless enhanced-beacon-table [enable|erase-report]
service wireless enhanced-beacon-table channel-set
  [a|an|bg|bgn] <1-200>
service wireless enhanced-beacon-table max-ap <0-512>
service wireless enhanced-beacon-table scan-interval <10-60>
service wireless enhanced-beacon-table scan-time <100-1000>

service wireless enhanced-probe-table [enable|erase-
report|max-mu|preferred|window-time]
service wireless enhanced-probe-table [enable|erase-report]
service wireless enhanced-probe-table max-mu <0-512>
service wireless enhanced-probe-table preferred <MAC>
service wireless enhanced-probe-table window-time <10-60>

service wireless free-packet-watermark <0-100>
service wireless idle-radio-send-multicast enable
service wireless map-radios <1-127>
service wireless radio-misc-cfg <hex-mask>
service wireless request-ap-log <ap-index>
```

`service wireless snmp-trap-throttle` `<1-20>`
`service wireless vlan-cache` `enable`

Parameters (Privilege Executable Mode)

clear [all|aplogs|clitree|cores| dumps|fw|panics| snooptable|wireless]	Performs a variety of reset functions • all – Removes all core, dump and panic files • aplogs – Removes all AP log files • clitree – Removes clitree.html (created by the save-cli command) • cores – Removes all core files • dumps – Removes all dump files • fw flows – Clears firewall sessions • flows – Firewall established sessions • panics – Removes all kernel panic files • securitymgr flows – Securitymgr parameters • flows [<0-349>|ge me1|sa|vlan|all] – Sessions established • <0-349> – Flow Index • WORD – Interface name • all – All established sessions • vlan <1-4094> – VLAN • me1 - Fast Ethernet interface • sa <1-4> – Static Aggregate interface • ge <1-4> – Gigabit Ethernet interface • snooptable – Clear Static and Dynamic Snoop entries • wireless – wireless related parameters • mobile-unit association-statistics– Clears mobile unit related parameters • association-statistics – Clears association and reassociation statistics

copy tech-support [<file>|<URL>] [tftp|ftp|sftp]	Copies files for tech support purposes • tech-support [<file>|<URL>] [tftp|ftp|sftp] – Copies extensive system information useful to technical support for troubleshooting. • FILE – File to which to copy • cf:/path/file • usb1:/path/file • usb2:/path/file • URL– Target URL from which to copy • tftp://<hostname:port or IP>/path/file • ftp://<user>:<passwd>@ <hostname:port or IP>/path/file • sftp://<user>@<hostname:port or IP>/path/file
dhcp-snoop-conflict-detection disable	IP Address, MAC Address conflict detection based on DHCP Snoop Table • disable – Disable packet drop based on conflict detection

diag [enable|identify| limit|period| tech-support-period| tech-support-url]	Sets or displays switch diagnostic values • enable – Enables in-service diagnostics • fanduty <40-100> – CPU fan PWM duty cycle. Set a value between 40-100%. Setting a value below 60 is considered unreliable. • identify – Identifies a switch by flashing the LEDs • limit [buffer|fan|filesys|inodesload|maxFDs |pkbuffers|procRAM|ram|routechache|temperature] – Diagnostic limit commands • buffer [] – Configures the buffer usage warning limit. The warning limit can be set to the buffer limit size of [128|128k|16k|1k|256|2k|32|32k|4k|512|64| 64k|8k] • fan <1-3> low <1000-150000> – Sets the fan speed limit for the fans on the switch. • low <1000-15000> – Sets limit value from 1000 to 15000 • filesys [etc2|flash|var] – Sets the file system freespace limit • inodes [etc2|flash|var] – Sets the file system inode limit • load [01|10|15] – Aggregate processor load • maxFDs <0-32767> – Configures the maximum number of file descriptors between 0 - 32767. • pkbuffers <0-65535>– Sets the packet buffer head cache limit between 0 - 65535. • procRAM <0.0-100.0> – Configures the RAM space used by a process. Set the percentage of RAM space between 0.0 and 100.0 percent . • ram <0.0-25.0> – Configures the free space for the RAM. Configure the free space between 0.0 and 25.0 percent.

	• routecache <0-65535> – Configures IP route cache usage. Set between 0 and 65553. • temperature <1-6> [critical|high|low] – Sets the number of temperature sensors for the switch. • critical <0.0 - 250.0> – Critical temperature limit • high <0.0 - 250.0> – high temperature limit • low <0.0 - 250.0> – low temperature limit • period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milli seconds. The default value is 1000 milliseconds.
diag-shell	Provides diag shell access
encrypt[secret|2| <pass-phrase>| <encryption-key>]	Encrypt password or key with secret • secret – Encrypt passwords/keys with secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Passphrase for encryption • <encryption-key> – Plaintext password or key to encrypt
firewall disable	Configures firewall parameters • disable – Disable firewall
kill connection *{<1-64>}*	Kills a connection using ESPI Adapter index • connection <1-64> – A single optional ESPI Adapter index

pktcap on [bridge|interface|router|vpn] [count|filter|verbose|write]	Packet capturing • on – Defines the packet capture location • bridge [count|hex|snap|verbose|write|filter] – Captures packet at the bridge • count <1-1000000> – Limits the captured packet count • filter [<LINE>|arp|capwap|dst|ether|host|icmp|igmp|ip|ip6|l2|l3|l4|net|not|port|src|tcp|udp|vlan|wlan] – Filters packets based on specified criteria. • <LINE> – Defines user defined packet capture filter • arp – Match arp packets • capwap – Match Capwap packets • dst – Match IP destination • ether – Ethernet • host – Match IP address • icmp – Match icmp packets • igmp – Match igmp packets • ip – Match IPV4 packets • ip6 – Match IPV6 packets • l2 – Match L2 header • l3 – Match L3 header • l4 – Match L4 header • net – Match IP in subnet • not – Logical not • port – Match TCP or UDP port • src – Match IP source • tcp – Match TCP packets • udp – Match UDP packets • vlan – Match vlan • wlan – Match wlan

	• verbose <1-1000000> – Displays full packet body • filter – Captures the filter • snap <1-1518>– Captured data length • write [<FILE>|URL] – Captures to a file • FILE – File to which to copy • cf:/path/file • usb1:/path/file • usb2:/path/file • URL– Target URL from which to copy • tftp://<hostname:port or IP>/path/file • ftp://<user>:<passwd>@ <hostname:port or IP>/path/file • sftp://<user>@<hostname:port or IP>/path/file • interface [<WORD>|ge|me1|sa|vlan] – Captures at an interface • WORD – Interface name • ge <1-4> – Gigabit Ethernet interface • me1 – Fast Ethernet interface • sa <1-4> – Static Aggregate interface • vlan <1-4094> – VLAN • count – Limits capture packet count • filter – Filters on criteria • inbound – Captures inbound packets only • outbound – Captures outbound packets only • verbose – Displays full packet body • write – Captures to a file • snap – Captured data length • hex – Show full packet body • router [counter|filter|verbose|write|snap|hex] – Captures packets at the router.

	• count <1-1000000> – Limits capture packet count • filter – Captures filter • verbose – Displays full packet body • write – Captures to a file • snap <1-1518> – Captured data length • hex – Show full packet body • count – Limits capture packet count • filter – Captures the filter • snap – Captured data length • vpn – Captures at the VPN • count – Limits capture packet count • filter – Captures the filter • inbound – Captures ingress direction only • outbound – Captures egress direction only • verbose – Displays full packet body • write – Captures to a file • snap – Captured data length • hex – Show full packet body • count – Limits capture packet count • filter – Captures the filter • snap – Captured data length
pm stop	Process Monitor • stop – Stops the PM from monitoring all daemons
save-cli	Saves the CLI tree for all modes in HTML
securitymgr [disable| disable-flow-rate-limit| dump-core| enable-http-stats]	Securitymgr parameters • disable – Disables securitymgr • disable-flow-rate-limit – Disables flow rate limiting • dump-core – Creates a core file of the securitymgr process • enable-http-stats – Enables the securitymgr HTTP statistics interface

show [cli| command-history| crash-info|diag|fw|info| ip|last-passwd|memory| pm|process| reboot-history|rtls| securitymgr|smart-rf| startup-log| upgrade-history| watchdog|wireless]	Displays running system information • cli – Shows the CLI tree of the current mode • command-history – Displays a command (except show commands) history • crash-info – Displays information about core, panic and AP dump files • diag [hardware|period|limits|stats|tech-support-period|tech-support-url|top] – Displays diagnostics • hardware – Displays the hardware system configuration • period – Displays the period (ms) for the in service diagnostics • limits – Displays limits value • stats – Displays current diagnostics statistics • tech-support-period – Displays the tech-support period (minutes) for the in service diagnostics • tech-support-url – Displays the tech-support-url • top –Displays top processes • fw flows – Firewall • flows brief– Sessions Established • brief – Summary of active flows • info – Shows a snapshot of available support information • last-passwd – Displays the last password used to enter the shell • memory – Shows memory statistics

	• pm history – Process Monitor • history [WORD|all] – Displays state changes for a process, the time they happened and events • WORD – Process name • all – All processes • process – Shows processes (sorted by memory usage) • reboot-history – Shows a reboot history • rtls [grid|location-history|rfid] – Locationing Configuration • grid [all|x] – Displays RSSI values in grid • all – Displays all grids • x <0-9000> – Displays grid x coordinates • y<0-9000> – Displays grid y coordinates • location-history [events] – Displays location engine history • rfid [events]– RFID Configuration • events <1-48> – Displays RFID reader events • <1-48> – A single RFID reader index • securitymgr – Security manager information displays • smart-rf [debug-config| sensitivity] – Smart-RF Management commands • debug-config – Displays smart-rf debug configuration • sensitivity [mu|pattern|rates] – Displays sensitivity table • mu[<1-8192>|WORD]– for given mu • <1-8192> – A single index • WORD – MAC address of mu-cache entry to show • pattern|rates – for common mu pattern • startup-log – Shows the startup log • upgrade-history – Shows an upgrade history • watchdog – Shows the watchdog status • wireless – Displays wireless parameters

show securitymgr flows	Service Security Manager parameters • flows [details|source] – Sessions established • details – Shows detail flow statistics • source [A.B.C.D|any] – Shows the source IP address • [A.B.C.D|any] – Flows where source address is A.B.C.D or flows with any source address • destination [A.B.C.D|any] – Destination IP address • [A.B.C.D|any] – Flows where the destination address is A.B.C.D or flows with any destination address • protocol [any|icmp|tcp|udp] – Protocol type • [any|icmp|tcp|udp] – Flows having any or icmp or tcp or udp protocol

smart-rf [clear-history|load-from-file|replay|rescue|restore|save-to-file|simulate]	Displays Smart-RF Management Commands • clear-history– clears assignment history • load-from-file – load record from file • replay enable – set replay mode • enable – enable replay mode • rescue <MAC> – force rescue operation • <MAC> – A single radio-mac-address, a single index • restore <MAC> – remove any recovering operation on given mode • <MAC> – A single radio-mac-address a single index • save-to-file – save records to file smart.bin • simulate [coverage-hole|interference] – Simulate radio events • coverage-hole <1-4096> – Simulate coverage hole • experienced-rate transmit-rate – Provide the experienced rate in mbps • transmit-rate [patter-11a|pattern-11b|pattern-11bg|pattern-2-mbps] – Provide the simulated MU's allowed transmit rates in hexadecimal format • pattern-11a – 11a Unit • pattern-11b – 11b Unit • pattern-11bg – 11bg Unit • pattern-2-mbps – 2 Mbps Unit • interference <MAC> – Simulate interference on radio • <MAC> – A single radio-mac-address, a single index
start-shell	Provides shell access
test	Provides test parameters
undefine ecspec <SPECNAME>	Undefines non active Event Cycle Specification • ecspec <SPECNAME> – Name of ECSpecs configuration

watchdog	Enables the switch watchdog
wireless [ap-history| clear-ap-log |custom-cli|dot11i| dump-core| enhanced-beacon-table| enhanced-probe-table| free-packet-watermark |idle-radio-send-multicast| legacy-load-balance |map-radios| radio-misc-cfg |rate-scale| request-ap-log |save-ap-log |snmp-trap-throttle| sync-radio-entries| vlan-cache]	Wireless parameters • ap-history [clear|enable] – Access-port history • clear – Delete all history of all APs • enable – Enable the tracking of AP history • clear-ap-log <1-1024> – Clears the AP logs • custom-cli [sh-wi-mobile-unit|sh-wi-radio] – Customize the output of some summary cli commands in wireless • sh-wi-mobile-unit [ap-locn|ap-name|channel| dot11-type|ip|last-heard|mac|radio-bss| radio-desc|radio-id|ssid|state|username|vlan |wlan-desc|wlan-id|username] – Customize the output of the "show wireless mobile-unit' command • ap-locn – The location of the AP where the mobile-unit is associated • ap-name – The name of the AP where the mobile-unit is associated • channel – The channel of the radio where the mobile-unit is associated • dot11-type –The dot11 radio type of the mobile-unit • ip – The IP address of the mobile-unit • last-heard – the time when a packet was last received from the mobile-unit • mac – MAC address of mobile-unit • radio-bss – the bssid of the radio where the mobile-unit is associated

	• radio-desc – description of radio where the mobile-unit is associated • radio-id – The radio index to which the mobile-unit is associated • ssid – The ssid of the mobile-units wlan • state – The current state of the mobile-unit • username – The Radius username of the user connected through this device (shown only if applicable and available) • vlan – The vlan-id assigned to the mobile-unit • wlan-desc – The wlan description the mobile-unit is using • wlan-id – The wlan index the mobile-unit is using • sh-wi-radio [adopt-info|ap-locn|ap-mac| ap-name|bss|channel|dot11-type|num-mu|power| radio-desc|radio-id|state] – Customize the output of the "show wireless radio" command • adopt-info – The adoption information about the radio • ap-locn – The location of the AP to which this radio belongs • ap-mac – The MAC address of AP to which the radio belongs • ap-name – The name of the AP to which this radio belongs • bss – The bssid of the radio • channel –The configured and current channel of the radio • dot11-type – The the dot11 type (11a/11g etc) of the radio

	• num-mu – The number of mobile devices associated with this radio • power – The configured and current transmit power of the radio • pref-id – The adoption preference id of the radio • radio-desc – The description of the radio • radio-id – The radio index in configuration • state – The current operational state of the radio • dot11i – modify dot11i service parameters • dump-core – Creates a core file of the ccsrvr process • enhanced-beacon-table [channel-set|enable| erase-report|max-ap|scan-interval|scan-time]– Enhanced beacon table for AP locationing. • channel-set [a|an|b|bg|bgn] <1-200> – Adds channels to the different radio types. Channel types are a, an, b, bg, bgn. The channel number must be in the range 1 to 200. • enable – Enables the Enhance Beacon Table feature for AP locationing • erase-report – Erases the reports for Enhanced Beacon Table feature. • max-ap <0-512> – Sets the maximum number of APs to be recorded in the Enhanced Beacon Table. Set a value in the range 0 -512. • scan-interval <10-60>– The time duration between two enhanced beacon table for AP locationing scans in seconds. • scan-time <100-1000>– The time duration of an Enhanced Beacon Table scan in millisecond.s

	• enhanced-probe-table [enable|erase-report|max-mu| preferred|window-time] – Enhanced probe table for MU locationing. • enable – Enables the Enhanced Probe Table feature for MU locationing. • erase-report – Erases the reports for Enhanced Probe Table feature. • max-mu <0-512> – Sets the maximum MUs in the Enhance Probe Table report. • preferred <MAC> – Add the MAC <MAC> to the preferred MU list. • window-time – Sets the Window Time for probe collection in seconds to a value in the range 10 to 60 seconds.
	• free-packet-watermark – It is free packets threshold. If the percentage of free packets is lower than this number, then additional packets will not be queued up in the datapath • idle-radio-send-multicast – Forward multicast packets to radios without associated mobile units • legacy-load-balance – Invoke legacy load balance algorithm • map-radios – Set radio-to-cpu mapping constant • radio-misc-cfg – radio specific misc configuration U16 for all radios • rate-scale – Enable wireless rate scaling (default) • request-ap-log – Request ap Log • save-ap-log – Saves debug/error logs sent by the access-port • snmp-trap-throttle – Limits the number of SNMP traps generated from the wireless module • sync-radio-entries – sync radio configuration at cluster levels • vlan-cache – VLAN-cache mode

```
service [advanced-vty|dhcp|diag|password-encryption|pm|
  prompt|radius|redundancy|set|show|terminal-length|
  watchdog]
service [advanced-vty|dhcp|watchdog]

service diag [enable|limit|period|tech-support-period|
  tech-support-url]
service password-encryption secret 2 <pass-phrase>
service pm sys-restart
service prompt crash-info
service radius {restart}
service redundancy dynamic-ap-load-balance start
service set [command-history|reboot-history|upgrade-history]
  <10-100>
service show cli
service terminal-length <0-512>
```

Parameters (GLOBAL Config)

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server
diag[enable|limit|period| tech-support-period| tech-support-url]	Displays diagnostics • enable – Enables in-service diagnostics • limit – Diagnostic limit command • period – Sets the diagnostics period • tech-support-period – Sets diagnostics tech-support-period • tech-support-url – Sets the URL to use during auto generated technical support dumps
password-encryption [secret|2|<pass-phrase> |<encryption-key>]	Encrypts passwords • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • <pass-phrase> – Passphrase for encryption • <encryption-key> – Plaintext password or key to encrypt

pm sys-restart	Process Monitor • sys-restart – Enables the PM to restart the system when a processes fails
prompt crash-info	Enable crash-info prompt • crash-info – Enables a crash-info prompt
radius restart	Enable radius server • restart – Restarts the radius server with an updated configuration
redundancy dynamic-ap-load-balance start	Configure redundancy group parameters • dynamic-ap-load-balance start – Enables the Dynamic AP Load Balance feature • start – Start dynamic AP load balance
set [command-history |reboot-history| upgrade-history]	Set service parameters. • command-history <10-300> – Sets the size of the command history (default is 200) • reboot-history <10-100> – Sets the size of the reboot history (default is 50) • upgrade-history <10-100> – Sets the size of the upgrade history (default is 50)
show	Shows running system information • cli – Shows the CLI tree of the current mode
terminal-length <0-512>	System wide terminal length configuration • <0-512> – Number of lines of VTY (0 means no line control)
watchdog	Enables the watchdog

Usage Guidelines

The `service password-encryption` set by the user cannot be disabled without knowing the old password. Refer the note below for more clarification.



NOTE: The `no service password-encryption` command used to disable the encryption, now requires the user to know the old password. The user will have to enter the old password to disable the encryption.

Earlier, using `no service password-encryption` disabled the encryption and `show running config` displayed the passwords as plaintext.

Now, the user has to user `no service password-encryption <old password key>` to disable or change the password.

Example

```
RFSwitch#service diag ?
 enable Enable in service diagnostics
 led   LED control
 limit  diagnostic limit command
 period Set diagnostics period

RFSwitch#service diag enable


RFSwitch#service diag led ?
 1 1 - upper LED
 2 2 - lower LED

RFSwitch#service diag led 1 ?
 amber amber
 blue  blue
 red  red

RFSwitch#service diag led 1 amber ?
 flashing LED Flashing
 off    LED off
 on    LED on.

RFSwitch#service diag led 1 amber flashing
RFSwitch#service diag led 1 amber flashing
RFSwitch#service diag led 1 blue on
RFSwitch#service diag led 1 red off
```

```
RFSwitch#service diag led 2 amber flashing

RFSwitch#service diag limit ?
 buffer    buffer usage warning limit
 fan     Fan speed limit
 filesys   file system freespace limit
 load     agregate processor load
 maxFDs    maximum number of file descriptors
 pkbuffers  packet buffer head cache
 procRAM   percent RAM used by a process
 ram     percent free RAM
 routecache  IP route cache usage
 temperature temperature limit

RFSwitch#service diag limit buffer ?
 128  128 byte buffer limit
 128k 128k byte buffer limit
 16k  16k byte buffer limit
 1k  1k byte buffer limit
 256  256 byte buffer limit
 2k  2k byte buffer limit
 32  32 byte buffer limit
 32k  32k byte buffer limit
 4k  4k byte buffer limit
 512  512 byte buffer limit
 64  64 byte buffer limit
 64k  64k byte buffer limit
 8k  8k byte buffer limit


RFSwitch>service show command-history

Configured size of command history is 200

 Date & Time     User Location  Command
============================================================
May 31 21:57:44 2007  admin   vty 130   exit
May 31 20:30:11 2007  admin   vty 130   configure terminal
May 31 20:27:08 2007  admin   vty 130   enable
May 31 20:18:03 2007  admin   vty 130   exit
May 31 20:17:32 2007  admin   vty 130   configure terminal
May 31 20:17:26 2007  admin   vty 130   enable
May 31 18:32:42 2007  admin   con 0   ip address 10.10.10.2/
24
May 31 18:32:29 2007  admin   con 0   interface vlan 1
```

```
May 31 18:31:48 2007  admin   con 0   configure terminal
May 31 18:31:45 2007  admin   con 0   enable
May 29 15:40:04 2007  admin   vty 131  enable
May 29 15:23:43 2007  admin   con 0   exit
May 29 15:23:36 2007  admin   con 0   ip address 10.10.10.2/
24
May 29 15:23:19 2007  admin   con 0   exit
May 29 15:23:19 2007  admin   con 0   exit
May 29 15:23:03 2007  admin   con 0   interface vlan 1
May 29 15:22:48 2007  admin   con 0   configure terminal
May 29 15:22:45 2007  admin   con 0   enable
May 25 21:32:27 2007  admin   vty 131   configure terminal
May 25 21:32:21 2007  admin   vty 131   enable
May 24 18:34:36 2007  admin   vty 131   configure terminal
May 24 18:34:21 2007  admin   vty 131   enable
May 23 19:07:35 2007  admin   vty 131   configure terminal
May 23 19:06:59 2007  admin   vty 131   enable
May 23 14:36:09 2007  admin   vty 130   enable
May 21 16:37:13 2007  admin   vty 130   enable
May 21 16:34:36 2007  admin   con 0    enable
```

RFSwitch>service show reboot-history

```
Configured size of reboot history is 50

 Date & Time       Event
==================================================
May 31 18:29:42 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 31 15:42:23 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 31 12:35:18 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 30 17:15:13 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 29 15:10:51 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 28 20:06:31 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 25 14:21:35 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 24 14:20:09 2007   startup
- - -          shutdown (ungraceful:unexpected cold restart)
May 23 14:07:21 2007   startup
- - -          shutdown (ungraceful:unexpected cold
```

2.2 show

Common Commands

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display_parameter, it displays information about that component.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show <parameter>
```

Parameters

Display Parameters	*Description*	*Mode*	*Example*
autoinstall	Displays the autoinstall configuration	Common	*page 2-42*
banner	Displays the message of the day login banner	Common	*page 2-43*
commands	Displays command lists	Common	*page 2-44*
crypto	Displays current encryption details	Common	*page 2-45*
environment	Displays environmental information	Common	*page 2-49*
history	Displays the session command history	Common	*page 2-49*
interfaces	Displays the current interface status and configuration	Common	*page 2-50*

Display Parameters	***Description***	***Mode***	***Example***
ip	Displays the internet protocol	Common	*page 2-52*
ldap	Displays the LDAP server configuration	Common	*page 2-59*
licenses	Displays the installed licenses, if any	Common	*page 2-61*
logging	Displays the logging configuration and buffer	Common	*page 2-62*
mac	Displays the media access control IP configuration	Common	*page 2-63*
mac-address-table	Displays the MAC address table	Common	*page 2-64*
management	Displays L3 management interface name	Common	*page 2-65*
mobility	Displays mobility parameters	Common	*page 2-66*
ntp	Displays network time protocol information	Common	*page 2-69*
port-channel	Displays port channel commands	Common	*page 2-71*
power	Displays power over ethernet command	Common	*page 2-72*
privilege	Displays the current privilege level	Common	*page 2-73*
radius	Displays RADIUS configuration commands	Common	*page 2-74*
redundancy dynamic-ap-load-balance	Display configuration details for dynamic AP Load Balance	Common	*page 2-75*

Display Parameters	***Description***	***Mode***	***Example***
redundancy - group	Displays redundancy group parameters	Common	*page 2-76*
redundancy-history	Displays the state transition history of the switch	Common	*page 2-79*
redundancy - members	Displays redundancy group members in detail	Common	*page 2-80*
rtls	Displays *Real Time Location System* (RTLS) commands	Common	*page 2-81*
smtp-notification	Displays trap enable flags (new)	Common	*page 2-84*
snmp	Displays SNMP engine parameters	Common	*page 2-86*
snmp-server	Displays SNMP engine parameters	Common	*page 2-87*
spanning-tree	Displays the spanning tree information	Common	*page 2-90*
static-channel-group	Displays static channel group membership information	Common	*page 2-92*
terminal	Displays terminal configuration parameters	Common	*page 2-93*
timezone	Displays the timezone	Common	*page 2-94*
traffic-shape	Displays traffic shaping configuration	Common	*page 2-95*
users	Displays information about terminal lines	Common	*page 2-96*
version	Displays software and hardware version information	Common	*page 2-97*
wireless	Displays wireless configuration commands	Common	*page 2-98*

Display Parameters	***Description***	***Mode***	***Example***
wlan-acl	Displays WLAN ACL information	Common	*page 2-112*
access-list	Displays the access list *Internet Protocol* (IP) configuration	Privilege/ Global Config	*page 2-113*
aclstats	Displays ACL statistics	Privilege/ Global Config	*page 2-114*
alarm-log	Displays all the alarms currently in the system	Privilege/ Global Config	*page 2-115*
boot	Displays the boot configuration	Privilege/ Global Config	*page 2-116*
clock	Displays the system clock	Privilege/ Global Config	*page 2-117*
debugging	Displays the current debugging settings	Privilege/ Global Config	*page 2-118*
dhcp	Displays DHCP server configurations	Privilege/ Global Config	*page 2-119*
file	Displays filesystem information	Privilege/ Global Config	*page 2-120*
ftp	Displays the FTP server configuration	Privilege/ Global Config	*page 2-121*
password-encryption	Displays password encryption data	Privilege/ Global Config	*page 2-122*
running-config	Displays the current operating configuration	Privilege/ Global Config	*page 2-123*
securitymgr	Displays debug information for ACL, VPN and NAT	Privilege/ Global Config	*page 2-127*
sessions	Displays currently open and active connections	Privilege/ Global Config	*page 2-128*

Display Parameters	***Description***	***Mode***	***Example***
startup-config	Displays the content of the startup configuration	Privilege/ Global Config	*page 2-129*
upgrade-status	Displays the status of the last image upgrade	Privilege/ Global Config	*page 2-131*
mac-name	Displays the configured MAC names for this device	Privilege/ Global Config	*page 2-132*
access-list	Displays the access list information	Privilege/ Global Config	*page 2-133*
aclstats	Displays the ACL statistics for a particular WLAN	Privilege/ Global Config	*page 2-134*
alarm-log	Displays the alarm log on the device	Privilege	*page 2-135*
firewall	Displays wireless firewall	Common	*page 2-137*
role	Configures role parameters	Common	*page 2-138*

2.2.1 autoinstall

Common to all modes

Displays the autoinstall configuration information.

Syntax

```
show autoinstall status
```

Parameters

status	Displays status of autoinstall

Example

```
RFSwitch>show autoinstall
RFSwitch>feature  enabled   URL
config    yes    --not-set--
cluster cfg yes    --not-set--
image    yes    --not-set--
expected image version --not-set--

RFSwitch>
```

2.2.2 banner

▸ *Common to all modes*

Displays the message of the day string. This string can be used to alert the user to specific information that might be of interest.

Syntax

```
show banner motd
```

Parameters

motd	Displays the *Message of the Day* banner

Example

```
RFSwitch>show banner motd
Welcome to CLI
RFSwitch>
```

2.2.3 commands

- *Common to all modes*

Displays the available commands for the current mode.

Syntax

```
RFSwitch>show commands
```

Parameters

None

Example

```
RFSwitch#show commands
 acknowledge alarm-log (all|<1-65535>)
 acknowledge alarm-log (all|<1-65535>)
 archive tar /create (FILE|URL) .FILE
 archive tar /create (FILE|URL) .FILE
 archive tar /table (FILE|URL)
 archive tar /table (FILE|URL)
 archive tar /xtract (FILE|URL) DIR
 archive tar /xtract (FILE|URL) DIR
 cd (DIR|)
 cd (DIR|)
 change-passwd
 clear aclstats
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear alarm-log (new|all|acknowledged|<1-65535>)
 clear arp-cache
 clear crypto ipsec sa (A.B.C.D |)
 clear crypto ipsec sa (A.B.C.D |)
 clear crypto isakmp sa ( A.B.C.D |)
 clear crypto isakmp sa ( A.B.C.D |)
 clear ip dhcp binding (*|A.B.C.D)
.................................................(contd)
RFSwitch#
```

2.2.4 crypto

▸ *Common to all modes*

Displays the encryption mode information.

Syntax

```
show crypto[ipsec|isakmp|key|map|pki]
show crypto ipsec[sa|
security-association|transformset]
show crypto isakmp[policy <1-10000>|sa]
show crypto keymy pubkey rsa
show crypto map[interface <interface-name>|tag <tag-name>]
show crypto pki[request <trustpoint-name>|trustpoints]
```

Parameters

ipsec [sa|securityassociation |transformset]	Displays the IPSEC policy • sa – IPSec security association • security-association lifetime – Security association • lifetime – Defines the lifetime • transformset <name> – Transformset • <name> – Defines the transform set name or all transform sets
isakmp [policy <1-10000>|sa]	Displays ISAKMP policies • policy <1-10000> – Displays the priority of all the isakmp policies • sa – All crypto ISAKMP security associations
key mypubkey rsa	Displays authentication key management • mypubkey rsa – Shows the public keys associated with the switch • rsa – Displays the RSA public keys
map [interface|tag]	Displays crypto maps • interface <interface-name> – Sets crypto maps for an interface • tag <tag-name> – Sets crypto maps with a given tag

pki [request|trustpoints]	Displays Public Key Infrastructure (PKI) commands • request <trustpoint-name> – Displays the certificate requests • trustpoints – Displays the trustpoints and their configuration

Usage Guidelines

The security engine periodically updates the IPSec and Isakamp statistics (every 60 seconds)

Example

```
RFSwitch(config)#show crypto pki request tptest
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwaDELMAkGA1UEBhMCaW4xEjAQBgNVBAgTCWthcm5hdGFr
YTES
MBAGA1UEBxMJYmFuZ2Fsb3JlMQ8wDQYDVQQKEwZzeW1ib2wxDDAKBgNVBAsT
A3dp
ZDESMBAGA1UEAxMJdGVzdC1jZXJ0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKB
gQC3qisZdTn7rKzv5TrGtKt7fwMwaYpgehyl52I4fDLZYY/
WTTTJFyKwW6s+Pq2R
mM9oiqX8mCZeSEIJIATpAVT2M5Ukb4Br9YQDcWHs84oXRJxKPeZ3WscBld2s
oPvK
ui1LoizZH9iqawmkXED1TFMBbDWiOcfnqQKn8Tddeax/
JQIDAQABoDMwMQYJKoZI
hvcNAQkOMSQwIjALBgNVHQ8EBAMCBLAwEwYDVR0lBAwwCgYIKwYBBQUHAwEw
DQYJ
KoZIhvcNAQEEBQADgYEAoJMylm3aaY1CnkOO5TbxB+qL4F4MKL6+o/
m0yRPqy/2S
gkk/
OwxHvc3TbA9WjbKkFWIDyqU7X0d+c8f9KogwxDwWHll2IBiTCtBAq6hpgKOv
Um9GFvMFps9XVkKtYttN3fer9tA+6xY9CKlr12mNGOYFHyVjMc3Pic0ODFiP
HAU=
-----END CERTIFICATE REQUEST-----

RFSwitch(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
 Server certificate configured
```

```
  Subject Name:
    Common Name:     Symbol Technologies
  Issuer Name:
    Common Name:     Symbol Technologies
 Valid From:  Sep 13 16:14:49 2006 GMT
 Valid Until: Sep 13 16:14:49 2007 GMT

Trustpoint :tptest
------------------------------------------------
 CA certificate configured
  Subject Name:
    Common Name:     monarch
    Organizational Unit: wid
    Organization:    symbol
    Location:      bangalore
    State:        karnataka
    Country:       in
    email:        testuser@domain.com
  Issuer Name:
    Common Name:     monarch
    Organizational Unit: wid
    Organization:    symbol
    Location:      bangalore
    State:        karnataka
    Country:       in
    email:        testuser@domain.com
 Valid From:  Sep 11 05:48:52 2006 GMT
 Valid Until: Sep 11 05:48:52 2007 GMT
```

2.2.5 environment

- *Common to all modes*

Displays the environmental information such as fan speed, ambient temperature inside the switch and CPU temperature.

Syntax

```
show environment
```

Parameters

None

Example

```
RFSwitch>show environment
  upwind of CPU temperature : 30.0 C
  CPU die temperature : 49.0 C
  left side temperature : 29.0 C
  by FPGA temperature : 28.0 C
  front right temperature : 26.0 C
  front left temperature : 26.0 C
  fan 1 fan     : 6480 rpm
  fan 2 fan     : 6600 rpm
  fan 3 fan     : 6420 rpm


RFSwitch>
```

2.2.6 history

- *Common to all modes*

Displays the command history

Syntax

```
show history
```

Parameters

None

Example

```
RFSwitch>show history
  1 admin
  2 enable
  3 con ter
  4 exit
  5 show autoinstall
  6 con ter
  7 show autoinstall
  8 show banner
  9 show banner motd
 10 show command
 11 show crypto
 12 show environment
 13 show history

RFSwitch>
```

2.2.7 interfaces

- *Common to all modes*

Displays the status of the different switch interfaces

Syntax

`show interfaces [WORD|ge|me1|sa|switchport|vlan]`

Parameters

show interfaces [WORD|ge|me1|sa| switchport|vlan]	Displays the interface name • WORD– Displays interface name • ge – Displays Gigabit Ethernet interface information • me1 – Displays fast ethernet information • sa – Displays Static Aggregate information • switchport – Displays native VLAN(s) and allowed VLAN information on switch ports • vlan[WORD|ge|me1| sa|vlan <1-4094> – Displays VLAN interface details

Usage Guidelines

Use the `show interface` command to display the administrative and operational status of all the interfaces or a specified interface

Example

```
RFSwitch#show interfaces eth 1
Interface eth1
 Hardware Type Ethernet, Interface Mode Layer 2, address is
00-a0-f8-65-ea-8e
 index=2001, metric=1, mtu=1500, (HAL-IF)
<UP,BROADCAST,RUNNING,MULTICAST>
 Speed: Admin Auto, Operational 10M, Maximum 1G
 Duplex: Admin Auto, Operational Half
 Switchport Settings: Mode: Access, Access Vlan: 2100
  input packets 0, bytes 0, dropped 0, multicast packets 0
  input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo
0, missed 0
  output packets 0, bytes 0, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat
0, window 0
```

```
RFSwitch#
RFSwitch(config)#show interfaces switchport eth1
Interface eth1
 Switchport Settings: Mode: Access, Access Vlan: 2100

RFSwitch(config)#show interfaces switchport vlan1
Interface vlan1
 Switchport Settings: Mode: Access, Access Vlan: 0
```

2.2.8 ip

- *Common to all modes*

Displays Internet Protocol (IP) related information

Syntax

```
show ip [access-group|arp|ddns|dhcp|
dhcp-vendor-options|domain-name|dos|http|igmp|interface|
name-server|nat|route|routing|ssh|telnet]
show ip access-group [<interface-name>|all|ge|me1|role|sa|
vlan <1-4094>]
show ip arp
show ip ddnsbinding
show ip dhcp[binding|class|pool|sharednetwork|snoop]
show ip dhcp-vendor-options
show ip domain-name
show ip dos [config|stats]
show ip http [secure-server|server]
show ip igmp snooping [mrouter|querier|vlan]
show ip interface [<interface-name>|brief|ge|me1|sa|vlan]
show ip name-server
show ip nat [interfaces|translations]
show ip nat translations [inside|outside|verbose]
show ip nat translations inside [source|destination]
show ip nat translations outside [source|destination]
show ip route [<IP>|<IP-prefix-len>|detail]
show ip routing
show ip ssh
show ip telnet
```

Parameters

access-group [<interface-name> |all|ge|me1|role|sa|> |vlan <1-4094>]	Displays the ACLs attached to an interface • <interface-name> – Enter the name of the interface to which the ACL is associated. access-group lists the details of the ACLs configured on the particular Layer 3 or Layer 2 interface. • vlan <1-4094> – Enter the name of the VLAN interface to which the ACL is associated • all – Display ACLs attached on all interfaces • ge <1-4> – Gigabit Ethernet interface • me1 – FastEthernet interface • role <role-name> – Specify role name • sa <1-4> – Static Aggregate interface
arp	Displays existing entries in the *Address Resolution Protocol* (ARP) table
ddns binding	Displays the DDNS configuration • binding – DNS address bindings
dhcp [binding|class|pool |sharednetwork|snoop]	Displays the DHCP server configuration • binding manual – DNS address bindings • manual – Static DHCP Address Bindings class – Configures the DHCP server class • pool – DHCP pool designation • sharednetwork – Shared network information • snoop table – Snoop Table entries
dhcp-vendor-options	DHCP Option 43 parameters received from DHCP server
domain-name	Displays domain name information
dos [config|stats]	Denial of Service configuration • config – Displays ip dos configuration • stats – Displays ip dos stats

http [secure-server|server]	*Hyper Text Transfer Protocol* (HTTP) • secure-server – Secure HTTP server • server – HTTP server
interface [<interface-name>|brief|ge|me1|sa|vlan]	Use the show ip interface command to display the administrative and operational status of all Layer-3 interfaces or a specified Layer-3 interface. • <interface-name> – Interface name • brief – Brief summary of the IP status and its configuration • vlan <1-4094> – VLAN Interface • ge <1-4>– GigabitEthernet interface • me1 – FastEthernet interface • sa <1-4> – Static Aggregate interface
igmp snooping [mrouter|querier|vlan]	Displays Internet Group Management Protocol • snooping – IGMP Snooping • mrouter – Displays Multicast Router • querier – Configure IGMP querier • vlan [<1-4094>|<vlan-list>] – Identify the vlan to use
name-server	Displays static and dynamic name-server entries
nat [interfaces|translations]	Displays Network Address Translation • interfaces – Displays NAT Configuration on interfaces • translations [inside|outside|verbose] – Displays NAT translations • inside [source|destination]– Inside • outside [source|destination] – Outside • source – Displays Source • destination – Displays Destination • verbose – Displays NAT Translations in real-time

route [<IP>|<IP/Mask> |detail]	Display IP routing table entries • <IP> – Network in the IP routing table • <IP/Mask> – Number of valid bits in the network prefix IP prefix <network>/<length>, e.g., 35.0.0.0/8 • detail – Displays the IP routing table in detail
routing	IP routing status
ssh	Secured Shell (SSH) server
telnet	Telnet server

Usage Guidelines

1. The interface and VLAN status is displayed as UP regardless of a disconnection. In such a case, shutdown the VLAN.

   a. Check the status of an interface and VLAN using:

   ```
   RFSwitch(config)#show ip interface brief
   Interface       IP-Address      Status        Protocol
   vlan1         157.235.208.69(DHCP) up        up
   vlan3         unassigned       up          up
   RFSwitch(config)#
   ```

   If the stauts of the VLAN is UP (even if eth1/eth2 is disconnected), shutdown the VLAN associated with eth1 using:

   ```
   RFSwitch(config-if)#show ip interface vlan 3 brief
   Interface       IP-Address      Status        Protocol
   vlan3         unassigned       up          up
   RFSwitch(config-if)#shutdown
   ```

   b. Check the stauts. Note that the VLAN has now been disassociated and the status is DOWN.

   ```
   RFSwitch(config)#show ip interface brief
   Interface       IP-Address       Status        Protocol
   vlan1        157.235.208.69(DHCP)  up          up
   vlan3         unassigned       administratively down down
   RFSwitch(config)#
   ```

2. The above example could also occur when a DHCP interface is disconnected. DHCP is not effected though, because it runs on a virtual interface and not on a physical interface. In this case, it is the physical interface that is disconnected not the virtual interface. When the ethernet interface comes back up, it will restart the DHCP client on any virtual interfaces (SVIs) of which the physical interface is a member port. This ensures if the interface was disconnected and reconnected to a different interface, it obtains a new IP address, route, name server, domain name etc.

Example

```
RFSwitch(config)#show ip access-group eth 1
Interface eth1
 Inbound IP Access List :
 Inbound MAC Access List :

RFSwitch(config)#show ip access-group vlan 1
Interface vlan1
 Inbound IP Access List :

RFSwitch(config)#show ip access-group eth2
Interface eth2
 Inbound IP Access List :
 Inbound MAC Access List :

RFSwitch#show ip dhcp binding
IP       MAC/Client-Id   Type    Expiry Time
--       -------------   ----    -----------

RFSwitch(config)#show ip dhcp class
!
ip dhcp class TestClass2
 option user-class MC900
!
ip dhcp class BlahBlahBlah
!
ip dhcp class ClassNameTest
 option user-class UserClassTest
!
ip dhcp class TestDHCPclass
!
ip dhcp class Add-DHCP-class1
!
ip dhcp class MonarchDHCPclas
 option user-class MC9000
```

```
!
ip dhcp class RFSwitchDHCPclass
 option user-class MC800
RFSwitch(config)#

RFSwitch#show ip dhcp pool
!
ip dhcp pool pl
!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30
!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

RFSwitch#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:

RFSwitch#show ip domain-name
 IP domain-lookup : Enable
 Domain Name  : motorola.com

RFSwitch#show ip http server
HTTP server: Running
Config status: Enabled

RFSwitch#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint

RFSwitch#show ip interface brief
Interface   IP-Address    Status   Protocol
vlan1     157.235.208.233  (DHCP)up  up
tunnel1    unassigned    up     up

RFSwitch#show ip interface tunnel 1 ?
 brief Brief summary of IP status and configuration
```

```
RFSwitch#show ip interface tunnel 1 brief
Interface   IP-Address    Status   Protocol
tunnel1    unassigned    up     up

RFSwitch#show ip interface vlan 1 brief
Interface   IP-Address    Status   Protocol
vlan1     157.235.208.233  (DHCP)up  up

RFSwitch#show ip name-server
157.235.3.195      dynamic
157.235.3.196      dynamic

RFSwitch#show ip routing
IP routing is on

RFSwitch(config)#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
    > - Active route, - Next-hop in FIB, p - stale info

S    1.1.0.0/16 [1/0] via 1.1.1.1 inactive
S    1.1.1.0/24 [1/0] via 1.1.1.2 inactive
S    10.0.0.0/8 [1/0] via 10.10.10.10 inactive
S    157.235.208.0/24 [1/0] via 157.235.208.246 inactive

RFSwitch#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22

RFSwitch#show ip telnet
Telnet server: enabled
Status: running
Port: 23
```

2.2.9 ldap

▸ *Common to all modes*

Displays LDAP information

Syntax

```
show ldap configuration [primary|secondary]
```

Parameters

ldap configuration [primary|secondary]	Displays LDAP information. • Configuration [primary|secondary] – Sets the LDAP configuration server parameters • primary – Defines the Primary LDAP server • secondary – Defines the Secondary LDAP server

Example

```
RFSwitch(config-radsrv)#show ldap configuration
LDAP Server Config Details

Primary LDAP Server configuration

    IP Address       : 10.10.10.1
    Port          : 369
    Login         :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
    Bind DN       :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
    Base DN       : ou=symbol,dc=activedirectory,dc=com
    Password       : 0 symbol@123
    Password Attribute   : UserPassword
    Group Name       : cn
    Group Membership Filter:
(&(objectClass=group)(member=%{Ldap-UserDn}))
    Group Member Attr   : radiusGroupName
    Net timeout      : 1 second(s)

Secondary LDAP

    IP Address       : 10.10.10.5
    Port          : 369
    Login         :
```

```
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
    Bind DN         :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
    Base DN         : ou=symbol,dc=activedirectory,dc=com
    Password         : 0 symbol@123
    Password Attribute    : UserPassword
    Group Name        : cn
    Group Membership Filter:
(&(objectClass=group)(member=%{Ldap-UserDn}))
    Group Member Attr    : radiusGroupName
    Net timeout       : 1 second(s)
```

2.2.10 licenses

- *Common to all modes*

Displays the different licenses installed on the switch

Syntax

```
show licenses
```

Parameters

None

Example

```
RFSwitch(config)#show licenses
feature usage license string       license value  usage
AP       2FFD7fE9 CD016155 14A92C70 48     1
```

2.2.11 logging

- *Common to all modes*

Displays logging status and other information

Syntax

```
show logging
```

Parameters

None

Example

```
RFSwitch(config)#show logging

Logging module: enabled
  Aggregation time: disabled
  Console logging: level debugging
  Buffered logging: level informational
  Syslog logging: level debugging
    Facility: local7
    Logging to: 157.235.203.37
    Logging to: 10.0.0.2

Log Buffer (6520 bytes):

Sep 14 19:11:59 2006: %DAEMON-6-INFO: radiusd[4643]: Ready
to process requests.

Sep 14 19:11:58 2006: %PM-5-PROCSTOP: Process "radiusd" has
been stopped

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11a radio on AP
00-A0-F8-BF-8A-A2 adopted

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11bg radio on AP
00-A0-F8-BF-8A-A2 adopted
```

2.2.12 mac

▸ *Common to all modes*

Shows all MAC information with respect to groups and access lists

Syntax

```
show mac [access-list|access-group]
show mac access-group [<interface>|all|ge <1-4>|
me1|sa <1-4>|vlan <1-4094>]
```

Parameters

mac [access-list access-group]	Displays MAC information • access-list – Displays existing MAC access lists • access-group [<Interface>|all|ge <1-4>| me1|sa <1-4>|vlan<1-4094>] – Displays MACs access control lists (ACLs) attached the specified interface where: • <interface> – Name of the interface • all interfaces • ge <1-4> – The specified Gigabit interface • me1 – The fast ethernet interface • sa <1-4> – The specified Static Aggregate interface • vlan <1-4094> – VLAN • <1-4094> – Displays VID

Example

```
RFSwitch(config)#show mac access-list
RFSwitch(config)#show mac access-group all
```

2.2.13 mac-address-table

- *Common to all modes*

Displays the MAC address table entries

Syntax

```
show mac-address-table
```

Parameters

None

Example

```
RFSwitch(config)#show mac-address-table

Bridge    VLAN Port     Mac      Fwd
----------- ---- ----------- -------------- ---
1      10  ge1     00a0.f865.ea8f 1
1      10  ge1     0015.7038.0653 1
1      10  ge1     0015.7014.fec4 1
1      10  ge1     0015.7041.9f7f 1

RFSwitch(config)
```

2.2.14 management

- *Common to all modes*

Displays the L3 management interface name

Syntax

```
show management
```

Parameters

None

Example

```
RFSwitch>show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFSwitch>
```

2.2.15 mobility

- *Common to all modes*

Displays the mobility parameters

Syntax

```
show mobility [event-log|forwarding|global|
mobile-unit|peer|statistics]
show mobility event-log [mobile-unit|peer]
show mobility forwarding <MAC>
show mobility mobile-unit [MAC>|detail]
show mobility peer [<IP>|detail]
show mobility statistics <MAC>
```

Parameters

event-log[mobile-unit|peer]	Displays mobility event logs • mobile-unit – MU event logs • peer – Peer event logs
forwarding <MAC>	Displays and defines mobile units in the forwarding plane • <MAC> – MAC address of the mobile unit
global	Displays and defines global mobility parameters
mobile-unit [<MAC>| detail]	Mobile units in the mobility database • <MAC> – MAC address of the mobile unit • detail – Displays detailed information
peer [<IP>|detail]	Mobility peers • <IP> – IP address of Peer • detail – Displays detailed peer information
statistics <MAC>	Mobility statistics • <MAC> – MAC address of the mobile unit

Example

```
RFSwitch(config)#show mobility ?
 event-log  Event Log
 forwarding  Mobile-unit information in the forwarding plane
```

```
 global    Global Mobility parameters
 mobile-unit Mobile-units in the Mobility Database
 peer     Mobility peers
 statistics  Mobile-unit Statistics
```

RFSwitch(config)#show mobility event-log mobile-unit

```
Time      Event    Evt-Src-IP   MU-Mac       MU-IP
HS-IP      CS-IP
09/14 19:17:52 IP-UPD-MU  n/a       00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16 157.235.208.16
09/14 19:17:51 ADD-MU    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16
09/14 19:17:51 DEL-MU    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16
09/14 19:17:50 ADD-MU    n/a       00-0f-3d-e9-a6-54 0.0.0.0
157.235.208.16 157.235.208.16
```

RFSwitch>show mobility forwarding

```
Mobility Forwarding-plane Information
 State: HS : Home-switch    CS : Current-switch
     !HS: Not Home-switch  !CS: Not Current-switch
Mac-Address    IP-Address   State  HS-Vlan  Tunnel
RFSwitch>
```

RFSwitch>show mobility global

```
Mobility Global Parameters
Admin Status           : DISABLED
Operational-Status        : DISABLED (Admin-status is
DISABLED)
Local Address           : 10.10.10.2 (mgmt-vlan)
Port Number            : 58788
Max Roam Period          : 5 sec
Number of Peers          : 0 (established=0)
Number of MUs           : 0 (Home=0, Foreign=0, Delete-
pend=0)
L3-Mobility enabled WLANs     : NONE
RFSwitch>
```

RFSwitch(config)#show mobility mobile-unit detail

```
HOME MU Database: Total=1
MU MAC-Address: 00-0f-3d-e9-a6-54, IP-Address:
157.235.208.134,
SSID=wios_rad_test1
 Home-Switch: 157.235.208.16, Current-Switch:
157.235.208.16, HS-VLAN=1
```

```
Foreign MU Database: Total=0

RFSwitch(config)#show mobility peer detail
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
 Join-Sent : 0   Join-Rcvd : 0   Leave-Sent : 0   Leave-Rcvd
: 0
 Rehome-Sent: 0   Rehome-Rcvd: 0   L3roam-Sent: 0   L3roam-
Rcvd: 0
 Num-flaps : 0   Connect-retries: 0  Peer-Uptime: 0 days,
00:00:00

RFSwitch(config)#show mobility statistics

MU <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-------------------------------------------
Inter-     |Rx                     |Tx
face      |unicast  MC     BC     Error   |unicast  MC
BC     Error
wlan_port    0     0     0     0     0     0
0     0
```

2.2.16 ntp

▸ *Common to all modes*

Displays NTP protocol information

Syntax

```
show ntp [association|status]
```

Parameters

ntp [association detail|status]	Displays the *Network Time Protocol* (NTP) configuration • association detail – Displays existing NTP associations • detail – Displays NTP association details • status – Displays NTP status

Example

```
RFSwitch>show ntp associations
 address     ref clock    st when poll reach delay offset
disp
 * master (synced), # master (unsynced), + selected, -
candidate, ~ configured
RFSwitch>

RFSwitch>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000
Hz, precision is 2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC
2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFSwitch>

RFSwitch(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum
16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC
2036)
our mode client, peer mode unspec, our poll intvl 6, peer
poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
```

```
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2006)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
```

```
RFSwitch>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000
Hz, precision is 2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC
2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFSwitch>
```

2.2.17 port-channel

▸ *Common to all modes*

Displays port-channel load-balance information

- RFS7000



SWITCH NOTE: This command is not supported on:

- RFS6000

Syntax

```
show port-channel load-balance
```

Parameters

load-balance	Displays the existing load balancing configuration

Example

```
RFSwitch>show port-channel load-balance
RFSwitch>
```

2.2.18 power

Common to all modes

Displays the power configuration and status for the RFS6000 switch

Supported in the following platforms:

- RFS6000



SWITCH NOTE: This command is not supported on:

- RFS7000

Syntax

```
show power [configuration|status]
```

Parameters

configuration	Displays configuration of power over ethernet
status	Displays status of power over ethernet

Example

```
RFSwitch(config)#show power configuration

Power usage trap at 80% of max power (148 of 185 Watts)

 port Priority  Power limit Enabled
 ge1 high    29.7W    yes
 ge2 high    29.7W    yes
 ge3 high    29.7W    yes
 ge4 high    29.7W    yes
 ge5 high    29.7W    yes
 ge6 high    29.7W    yes
 ge7 high    29.7W    yes
 ge8 high    29.7W    yes

 POE firmware version 01f6 build 4

RFSwitch(config)#
```

2.2.19 privilege

- *Common to all modes*

Displays the privileges of the current user

Syntax

```
show privilege
```

Parameters

None

Example

```
RFSwitch>show privilege
Current user privilege: superuser
RFSwitch>
```

2.2.20 radius

- *Common to all modes*

Displays RADIUS status and information

Syntax

```
show radius [configuration|eap configuration|group|
nas  A.B.C.D/M|proxy|rad-user|trust-point]
```

Parameters

radius [configuration| eap configuration group| nas <IP/Mask>|proxy| rad-user|trust-point]	Displays RADIUS configuration commands • configuration – RADIUS server configuration parameters • eap configuration – Displays and defines the EAP configuration • group – Displays the RADIUS group configuration • nas <IP/Mask> – Defines a client IP address and mask • proxy – Lists proxy information • rad-user – Displays RADIUS user information • trust-point – Defines the RADIUS trust-point configuration

Example

```
RFSwitch(config)#show radius proxy
Proxy Details
_____________
Proxy retry delay : 6 seconds
Proxy retry count : 4

Proxy Realm Details
___________________
Realm  : symbol.com
    IP Address  : 10.10.10.5
    Port     : 1812
    Shared secret : 0 secret123
```

2.2.21 redundancy dynamic-ap-load-balance

▸ *Common to all modes*

Displays the configuration for the Dynamic AP Load Balancing feature

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show redundancy dynamic-ap-load-balance config
```

Parameters

config	Displays configuration details for dynamic AP load balance

Example

```
RFSwitch(config)#show redundancy dynamic-ap-load-balance config
Dynamic AP Load Balance Configuration:
 Load balance     : Enabled
 Load balance trigger : Schedule

Dynamic AP Load Balance Schedule:
 Schedule first-time  : Sun Jun 1 00:00:00 2008
 Schedule interval   : 1 day(s)

Per AP MU Threshold   : 32
RFSwitch(config)#
```

2.2.22 redundancy -group

▸ *Common to all modes*

This command displays the switch's IP address, number of active neighbors, group license, installed license, cluster AP adoption count, switch adoption count, hold time, discovery time, heartbeat interval, cluster id and switch mode.

In a cluster, this command displays the redundancy runtime and configuration of the "self-switch". Use `config` to view only configuration information and/or `runtime` parameters.

Syntax

```
show redundancy -group [config|runtime]
```

Parameters

redundancy -group [config | runtime]	Displays redundancy runtime and configuration details. • config – Displays configured redundancy group information • runtime – Displays runtime redundancy group information

Example

```
RFSwitch(config)#show redundancy -group

Redundancy Group Configuration Detail
Redundancy Feature         : Disabled
Redundancy group ID        : 1
Redundancy Mode          : Primary
Redundancy Interface IP      : 0.0.0.0
Number of configured peer(s)    : 0
Heartbeat-period          : 5 Seconds
Hold-period            : 15 Seconds
Discovery-period          : 30 Seconds
Handle STP             : Disabled
Switch Installed License      : 48
Switch running image version    : 3.1.0.0-008D
Auto-revert-period         : 5 mins
Auto-revert Feature        : Disabled
DHCP-Server Redundancy       : Disabled

Redundancy Group Runtime Information
```

```
Redundancy Protocol Version     : 2.0
Redundancy Group License       : 0
Cluster AP Adoption Count      : Not Applicable
Switch AP Adoption Count       : Not Applicable
Redundancy State           : Disabled
Radio Portals adopted by Group    : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group   : Not Applicable
Rogue APs detected by this Switch  : Not Applicable
MUs associated in this Group     : Not Applicable
MUs associated in this Switch    : Not Applicable
Selfhealing RPs in this Group    : Not Applicable
Selfhealing APs in this Switch    : Not Applicable
Group maximum AP adoption capacity  : Not Applicable
Switch Adoption capacity       : Not Applicable
Established Peer(s) Count      : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group         : Not Applicable

RFSwitch(config)#


RFSwitch(config)#show redundancy -group config

Redundancy Group Configuration Detail
Redundancy Feature         : Disabled
Redundancy group ID        : 1
Redundancy Mode          : Primary
Redundancy Interface IP      : 0.0.0.0
Number of configured peer(s)    : 0
Heartbeat-period          : 5 Seconds
Hold-period            : 15 Seconds
Discovery-period          : 30 Seconds
Handle STP             : Disabled
Switch Installed License      : 48
Switch running image version    : 3.1.0.0-008D
Auto-revert-period         : 5 mins
Auto-revert Feature        : Disabled
DHCP-Server Redundancy       : Disabled

RFSwitch(config)#

RFSwitch(config)#show redundancy -group runtime

Redundancy Group Runtime Information
```

```
Redundancy Protocol Version     : 2.0
Redundancy Group License       : 0
Cluster AP Adoption Count      : Not Applicable
Switch AP Adoption Count       : Not Applicable
Redundancy State           : Disabled
Radio Portals adopted by Group    : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group   : Not Applicable
Rogue APs detected by this Switch  : Not Applicable
MUs associated in this Group     : Not Applicable
MUs associated in this Switch    : Not Applicable
Selfhealing RPs in this Group    : Not Applicable
Selfhealing APs in this Switch    : Not Applicable
Group maximum AP adoption capacity  : Not Applicable
Switch Adoption capacity       : Not Applicable
Established Peer(s) Count      : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group         : Not Applicable

RFSwitch(config)#
```

2.2.23 redundancy-history

- *Common to all modes*

Displays the switch state transition history

Syntax

```
show redundancy -history
```

Parameters

None

Example

```
RFSwitch>show redundancy -history
State Transition History

Time         Event Triggered     state
-------------------------------------------------------
Sat Oct 06 12:07:55  Redundancy Enabled   Startup
Sat Oct 06 12.07.56   Startup Done         Discovery
Sat Oct 06 12:08:26  Discovery Done     Active
Sat Oct 06 22:10:10  Redundancy Disabled   Startup

RFSwitch>show
```

2.2.24 redundancy -members

▸ *Common to all modes*

Displays the member switches in the cluster. The user can provide the `IP address` of the switch in cluster whose information alone is needed.

Syntax

```
show redundancy-members [<IP>|brief]
```

Parameters

redundancy-members [<IP>|brief]	Displays member switches in the cluster • <IP>– Displays the IP addresses of member switches • brief – Displays members in brief

Example

```
RFSwitch(config)#show redundancy -members brief

Member ID (Self)       : 10.10.10.10
Member State          : Not Applicable

Member ID            : 10.10.10.1
Member State          : Peer Configured
```

2.2.25 rtls

- *Common to all modes*

Displays the Real Time Locating System status and information

Syntax

```
show rtls [aeroscout|espi|filter|ekahau|
reference-tags|rfid|site|sole|tags|zone]
```

Parameters

rtls [aeroscout|espi|filter|ekahau|reference-tags|rfid|site|sole|tags|zone]	Displays the Real Time Locating System status and information. • aeroscout – Displays aeroscout configurations • espi [adapter|ecspecs|subscriber|tags] – Displays ESPI configuration • adapter [active|ale-tcp] – Displays Adapter Configuration • active – Displays adapters that are currently active • ale-tcp – Displays ale-tcp adapter • ecspecs [<SPECNAME>|active|define|detail|requested] – Displays ecsspecs configuration • <SPECNAME> – Displays name of Ec Specs • active detail – Displays detailed active ECSpecs status • defined detail – Displays defined active ECSpecs status in detail • detail – Show detailed ECSpecs status • requested detail – Displays requested detailed ECSpecs status • subscriber – Displays info for given subscriber's IP • tags subscriber – Displays tags for given subscriber's IP • filter – Displays RFID tag filters • ekahau – Displays ekahau configurations • reference-tags – Displays reference tag configurations • rfid – Displays RFID configuration • site – Displays site configurations • sole – Displays SOLE configurations • zone <1-48> – Displays zone configuration

rtls tags [<tag-id>| aeroscout|all|ekahau|g2| mobile-unit| |rfid|uri|zone|]	Displays Tags/Assets (passive, active, wi-fi, uwb) Information • <tag-id> – Displays detailed tag information for specific tag ID • aeroscout – Displays located aeroscout tags • all – Displays all tags • ekahau – Displays located ekahau tags • g2 – Displays located g2 tags • mobile-unit – Displays located mobile units • rfid - Displays located RFID gen2 tags • uri <URI> – Displays RFID tags for given notification URI • zone <1-48> – Display zone configuration
zone [<1-48>|detail]	Displays logical reader statistics • <1-48> – Display zone configuration • detail – Displays zone details

Example

```
RFSwitch(config)#show rtls ?
 aeroscout    Aeroscout configurations
 espi      ESPI Configuration
 filter    RFID Tag Filters
 ekahau    Ekahau configurations
 reference-tags Reference tag Configurations
 rfid      RFID Configuration
 site      Site configurations
 sole      SOLE configurations
                Information
 zone      Show logical reader statistics
RFSwitch(config)#show rtls
```

2.2.26 smtp-notification

- *Common to all modes*

Displays the set smtp-notification parameters

Syntax

```
show smtp-notification traps
```

Parameters

traps	Displays trap enable flags

Example

```
RFSwitch(config)#show smtp-notification traps
-----------------------------------------------------------------
-Global enable flag for Trap SMTP-Notification      Disabled
-----------------------------------------------------------------
-Enable flag status for Individual Trap SMTP-Notification
-----------------------------------------------------------------
--Module Type        Trap Type         Enabled?[Y/N]
-----------------------------------------------------------------
--snmp            coldstart              N
snmp              linkdown               N
snmp              linkup                 N
snmp              authenticationFail     N
nsm               dhcpIPChanged          N
diagnostics       tempHigh               N
diagnostics       tempOver               N
diagnostics       fanSpeedLow            N
diagnostics       cpuLoad1Min            N
diagnostics       cpuLoad5Min            N
diagnostics       cpuLoad15Min           N
diagnostics       usedKernelBuffer       N
diagnostics       ramFree                N
diagnostics       processMemoryUsage     N
diagnostics       packetBuffers          N
diagnostics       ipRouteCache           N
diagnostics       fileDescriptors        N
redundancy        memberUp               N
redundancy        memberDown             N
```

```
redundancy        memberMisConfigured         N
redundancy        adoptionExceeded            N
redundancy        grpAuthLevelChanged         N
redundancy        resourceUp                  N
redundancy        resourceDown                N
misc           lowFsSpace                     N
misc           processMaxRestartsReached      N
misc           savedConfigModified            N
misc           serverCertExpired              N
misc           caCertExpired                  N
misc           periodicHeartbeat              N
misc           switchEvent                    N
wireless station     associated               N
wireless station     disassociated             N
wireless station     deniedAssociationOnCapability     N
wireless station     deniedAssociationOnShortPream     N
wireless station     deniedAssociationOnSpectrum       N
wireless station     deniedAssociationOnErr            N
wireless station     deniedAssociationOnSSID           N
wireless station     deniedAssociationOnRates          N
wireless station     deniedAssociationOnInvalidWPAWPA2IE    N
wireless station     deniedAssociationAsPortCapacityReached N
wireless station     tkipCounterMeasures          N
wireless station     deniedAuthentication         N
wireless station     radiusAuthFailed             N
wireless station     vlanChanged                  N
wireless radio      adopted                       N
wireless radio      unadopted                     N
wireless radio      detectedRadar                 N
wireless ap-detection  externalAPDetected         N
wireless ap-detection  externalAPRemoved          N
wireless self-healing  activated                  N
wireless ids       muExcessiveEvents              N
wireless ids       radioExcessiveEvents           N
.....................................................
.....................................................
RFswitch(config)#
```

2.2.27 snmp

- *Common to all modes*

Displays SNMP user information

Syntax

```
show snmp user [snmpmanager|snmpoperator|snmptrap]
```

Parameters

snmp user [snmpmanager| snmpoperator|snmptrap	Displays SNMP user information • snmpmanager – Shows SNMP manager information • snmpoperator – Shows SNMP operator information • snmptrap – Shows SNMP trap information

Example

```
RFSwitch>show snmp user snmpmanager
userName   access  engineId          Authentication
Encryption
snmpmanager  rw    800001848067458b6bd7157745 MD5       DES
RFSwitch>

RFSwitch>show snmp user snmpoperator
userName   access  engineId          Authentication
Encryption
snmpoperator ro    800001848067458b6bd7157745 MD5       DES
RFSwitch>

RFSwitch>show snmp user snmptrap
userName   access  engineId          Authentication
Encryption
snmptrap   rw    800001848067458b6bd7157745 MD5       DES
RFSwitch>
```

2.2.28 snmp-server

- *Common to all modes*

Displays SNMP server information

Syntax

```
show snmp-server traps wireless-statistics[mesh|mobile-unit|
radio|wireless-switch|wlan]
```

Parameters

traps wireless-statistics [mesh| mobile-unit| radio| wireless-switch|wlan]	Displays existing wireless-stats rate trap enabled flags • mesh – Displays existing mesh rate traps • mobile-unit – Displays existing mobile unit rate traps • radio – Displays existing radio rate traps • wireless-switch – Displays existing wireless switch rate traps • wlan – Displays existing WLAN rate traps

Example

```
RFSwitch>show snmp-server traps
-----------------------------------------------------------
-------
Global enable flag for Traps                  N
-----------------------------------------------------------
-------
Enable flag status for Individual Traps
-----------------------------------------------------------
-------
Module Type        Trap Type         Enabled?[Y/N]
-----------------------------------------------------------
-------
snmp              coldstart              N
snmp              linkdown               N
snmp              linkup                 N
snmp              authenticationFail     N
nsm               dhcpIPChanged          N
redundancy        memberUp               N
redundancy        memberDown             N
redundancy        memberMisConfigured    N
redundancy        adoptionExceeded       N
```

```
redundancy            grpAuthLevelChanged          N
misc                  lowFsSpace                   N
misc                  processMaxRestartsReached    N
wireless station      associated                   N
wireless station      disassociated                N
wireless station      deniedAssociationOnCapability     N
wireless station      deniedAssociationOnShortPream     N
wireless station      deniedAssociationOnSpectrum       N
wireless station      deniedAssociationOnErr            N
wireless station      deniedAssociationOnSSID           N
wireless station      deniedAssociationOnRates          N
wireless station      deniedAssociationOnInvalidWPAWPA2IE  N
wireless station      deniedAssociationAsPortCapacityReached
N
wireless station      tkipCounterMeasures          N
wireless station      deniedAuthentication         N
wireless station      radiusAuthFailed             N
wireless radio        adopted                      N
wireless radio        unadopted                    N
wireless radio        detectedRadar                N
wireless ap-detection  externalAPDetected          N
wireless self-healing  activated                   N
wireless ids          excessiveAuthAssociation     N
wireless ids          excessiveProbes              N
misc                  savedConfigModified          N
RFSwitch>

RFSwitch>show snmp-server traps wireless-statistics mobile-
unit
   pktsps-greater-than             disabled
   tput-greater-than               disabled
   avg-bit-speed-less-than         disabled
   avg-signal-less-than            disabled
   nu-percent-greater-than         disabled
   gave-up-percent-greater-than    disabled
   avg-retry-greater-than          disabled
   undecrypt-percent-greater-than  disabled
RFSwitch>

RFSwitch>show snmp-server traps wireless-statistics radio
   pktsps-greater-than             disabled
   tput-greater-than               disabled
   avg-bit-speed-less-than         disabled
   avg-signal-less-than            disabled
   nu-percent-greater-than         disabled
```

```
   gave-up-percent-greater-than       disabled
   avg-retry-greater-than             disabled
   undecrypt-percent-greater-than     disabled
   num-stations-greater-than          disabled
RFSwitch>

RFSwitch>show snmp-server traps wireless-statistics
wireless-switch
   pktsps-greater-than                disabled
   tput-greater-than                  disabled
   num-stations-greater-than          disabled
RFSwitch>

RFSwitch>show snmp-server traps wireless-statistics wlan
   pktsps-greater-than                disabled
   tput-greater-than                  disabled
   avg-bit-speed-less-than            disabled
   avg-signal-less-than               disabled
   nu-percent-greater-than            disabled
   gave-up-percent-greater-than       disabled
   avg-retry-greater-than             disabled
   undecrypt-percent-greater-than     disabled
   num-stations-greater-than          disabled
RFSwitch>
```

2.2.29 spanning-tree

- *Common to all modes*

Displays Spanning Tree information

Syntax

```
show spanning-tree mst [config|detail|instance]
show spanning-tree mst detail interface
[<interface-name>|ge|me1|sa|vlan <1-4094>]
show spanning-tree mst instance <1-15> interface
<IF NAME>||vlan <1-4094>}]
```

Parameters

config	Displays MST configuration information
detail interface [<interface-name>| ge <1-4>|me1|sa<1-4>| vlan <1-4094>]	Displays detailed interface information • <interface-name>– Displays the interface name • ge <1-4> – GigabitEthernet interface • me1 – FastEthernet interface • sa <1-4> – Static Aggregate interface • vlan (1-4094> – Defines the VLAN interface
instance <1-15> [<interface-name>| ge<1-4>|me1|sa<1-4>| vlan <1-4094>]	Displays instance information • <interface-name> – Displays the interface name • vlan <1-4094> – Defines the VLAN interface • ge <1-4> – GigabitEthernet interface • me1 – FastEthernet interface • sa <1-4> – StaticAggregate interface

Example

```
RFSwitch(config)#show spanning-tree mst config
%
% MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
% Format Id   : 0
% Name      : My Name
% Revision Level : 0
% Digest     : 0xAC36177F50283CD4B83821D8AB26DE62
```

```
%-----------------------------------------------------
RFSwitch(config)#

RFSwitch(config)#show spanning-tree mst detail interface eth
1
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000000000000
% 1: CIST Reg Root Id 8000000000000000
% 1: CST Bridge Id 800000a0f865ea8e
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco
interoperability off
%  eth1: Port 2001 - Id 87d1 - Role Disabled - State
Forwarding
%  eth1: Designated External Path Cost 0 -Internal Path Cost
0
%  eth1: Configured Path Cost 2000000 - Add type Explicit
ref count 1
%  eth1: Designated Port Id 0 - CST Priority 128 -
%  eth1: CIST Root 000000a0f865ea8e
%  eth1: Regional Root 000000a0f865ea8e
%  eth1: Designated Bridge 000000a0f865ea8e
%  eth1: Message Age 0 - Max Age 0
%  eth1: CIST Hello Time 0 - Forward Delay 0
%  eth1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello
Timer 0
%  eth1: Version Multiple Spanning Tree Protocol - Received
None - Send STP
%  eth1: No portfast configured - Current portfast off
%  eth1: portfast bpdu-guard default - Current portfast
bpdu-guard off
%  eth1: portfast bpdu-filter default - Current portfast
bpdu-filter off
%  eth1: no root guard configured   - Current root guard off
%  eth1: Configured Link Type point-to-point - Current
shared
%
RFSwitch(config)#
```

2.2.30 static-channel-group

▸ *Common to all modes*

Displays the members of the static channel groups

Supported in the following platforms:

- RFS7000



SWITCH NOTE: This command is not supported in:

- RFS6000

Syntax

```
show static-channel-group
```

Parameters

None

Example

```
RFSwitch(config)#show static-channel-group
RFSwitch(config)#
```

2.2.31 terminal

- *Common to all modes*

Displays the terminal information for the device

Syntax

```
show terminal
```

Parameters

None

Example

```
RFSwitch>show terminal
Terminal Type: vt102
Length: 44   Width: 125
RFSwitch>
```

2.2.32 timezone

- *Common to all modes*

Displays the timezone set on the device

Syntax

```
show timezone
```

Parameters

None

Example

```
RFSwitch>show timezone
Timezone is Etc/UTC
RFSwitch>
```

2.2.33 traffic-shape

▸ *Common to all modes*

Displays traffic shaping parameters

Supported in the following platforms:

- RFS7000



SWITCH NOTE: This command is not supported in:

- RFS6000

Syntax

```
show traffic-shape [config|priority-map|statistics]
```

Parameters

[config| priority-map| statistics]	• config class – Displays traffic shaping configuration • statistics class – Displays traffic shaping statistics • class <1-4> – Displays traffic shaping class number • priority-map – Displays .1p to transmit priority map

Example

```
RFSwitch(config)#show traffic-shape priority-map
 802.1p | Shaping priority
   0 | 2
   1 | 0
   2 | 1
   3 | 3
   4 | 4
   5 | 5
   6 | 6
   7 | 7
RFSwitch(config)#
```

2.2.34 users

- *Common to all modes*

Displays a list of users connected to the device

Syntax

```
show users
```

Parameters

None

Example

```
RFSwitch>show users
  Line   PID  User    Uptime    Location
  0 con 0 316  admin    06:08:11   ttyS0
 130 vty 0 2308  admin    00:35:18   0
RFSwitch>
```

2.2.35 version

- *Common to all modes*

Displays the current software & hardware version on the device

Syntax

```
show version {verbose}
```

Parameters

verbose	Displays software and hardware version information

Example

```
RFSwitch>show version
RFSwitch version 3.2.0.0-024D MIB=01a
Copyright (c) 2006-2007 Motorola, Inc.
Booted from secondary.

Switch uptime is 1 days, 20 hours 53 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
255844 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760
blocks, cache 0

RFS7000 version 1.3.0.0-018B MIB=01a
Copyright (c) 2006-2008 Motorola, Inc.
Booted from primary.

Switch uptime is 0 days, 1 hours 11 minutes
CPU is RMI XLR V0.4
PCI bus 0 device 3 function 2
  USB Controller
  unknown mfg
  unknown

PCI bus 0 device 1 function 0
  Ethernet controller
  unknown mfg
  unknown
255460 kB of on-board RAM
```

2.2.36 wireless

▸ *Common to all modes*



The `radio-group` range differs from switch to switch.

- RFS7000 – Supports a range between 0-255
- RFS6000 – Supports a range between 0-64

Displays the wireless configuration parameters and information

Syntax

show wireless [aap-version|ap|ap-containment|
ap-detection-config|ap-images|ap-unadopted|approved-aps|
channel-power|client|config|country-code-list|default-ap|fw|
hotspot|hotspot-config|ids|known|mac-auth-local|mesh|
mobile-unit|multicast-packet-limit|phrase-to-key|
qos-mapping|radio|radio-group|regulatory|self-heal-config
|sensor|smart-rf|unapproved-aps|wireless-switch-statistics|
wlan]
show wireless aap-version
show wireless ap[<1-48>|<MAC>|config [<1-1024>|<MAC>]
show wireless ap-containment [config|table]
show wireless ap-detection-config
show wireless ap-images
show wireless ap-unadopted
show wireless approved-aps
show wireless channel-power [11a|11b|11bg] [indoor|outdoor]
show wireless client [exclude-list|include-list]
show wireless config
show wireless country-code-list
show wireless default-ap
show wireless hotspot query
show wireless hotspot-config <1-32>
show wireless ids [filter-list|configured-bad-essids]
show wireless known *{ap statistics {<1-1024>}}*
show wireless mac-auth-local *{<1-1000>}*
show wireless mesh statistics *{<1-32> {detail}}*
show wireless mobile-unit ***{[<1-8192>|<MAC>|association-history|association-stats|probe-history|radio|roaming|statistics|voice|wlan]}***
show wireless mobile-unit [<1-8192>|<MAC>|association-stats]
show wireless mobile-unit association-history *{<MAC>}*
show wireless mobile-unit probe-history [<1-200>|config-list]
show wireless mobile-unit radio <1-4096>

```
show wireless mobile-unit roaming database
show wireless mobile-unit statistics [<1-4096>|<MAC>
{detail}|summary|voice [<1-4096>|<mac>]]
show wireless mobile-unit voice
show wireless mobile-unit vlan <1-256>
show wireless multicast-packet-limit
show wireless phrase-to-key [wep64|wep128] <pass-phrase>
show wireless qos-mapping {[wired-to-wireless|
wireless-to-wired]}
show wireless radio {[<1-4096>|admission-control|all|
beacon-table|config|monitor-table|statistics|unadopted|
uptime|voice]}
show wireless radio {[<1-4096>|all|beacon-table|monitor-
table|
unadopted|uptime]}
show wireless radio admission-control voice {<1-4096>}
show wireless radio config {[<1-4096>|default-11a|default-
11an|
default-11b|default-11bg|default-11bgn]}
show wireless radio statistics {[<1-4096> {detail}|
long-interval|short-interval|voice {[<1-4096>|long-interval|
short-interval]}}
show wireless radio voice {<1-4096>}
show wireless radio-group {<1-256>}
show wireless regulatory <country code>
show wireless self-heal-config {[<1-4096>|all]}
show wireless sensor {[<1-48>|default-config]}
show wireless smart-rf [calibration-status|configuration|
history|radio]
show wireless smart-rf radio [config|local-status|map|
master-status|neighbors|spectrum] {<1-4096>|<MAC>|
all-11a|all-llbg]}
show wireless unapproved-aps
show wireless wireless-switch-statistics {detail}
show wireless wlan [config {[<1-
256>|all|enabled]}|statistics {<1-256> {detail}}]
```

Parameters

aap-version	Displays the minimum adaptive firmware version string

ap [<1-48>|<MAC>| config [<1-48>|<MAC>]]	Status of the adopted access port • <1-48> – Defines the index of the access port • <MAC> – Sets the MAC address of a access port • config [<1-1024>|<MAC>] – Status of the configured access port. • <1-1024> – AP index from the "show wireless ap" command • <MAC> – MAC address of the ap.
ap-containment [config|table]	Rogue AP containment • config – Rogue AP Containment Parameters • table – Rogue AP Containment table
ap-detection-config	Detected AP configuration parameters
ap-images	Displays the access port images on the switch
ap-unadopted	Lists unadopted access ports
approved-aps	Displays approved APs detected by access port scans
channel-power [11a|11b|11bg] [indoor|outdoor]	Lists the channels and power levels available for a radio • 11a – Defines the radio as 802.11a • 11b – Defines the radio as 802.11b • 11bg – Defines the radio as 802.11bg These options are available for all the above radio types: • indoor – Radio is placed indoors • outdoor – Radio is placed outdoors
client [exclude-list|include-list]	Wireless client configuration • exclude-list – Sets the exclude list configuration • include-list – Sets the include list configuration
config	Displays wireless configuration information
country-code-list	Displays the list of supported country names and their 2 letter IS0 3166 codes

default-ap	Displays default access-port information
hotspot query	Displays hotspot query string configuration
hotspot-config <1-256>	WLAN hotspot configuration for specified index
ids [configured-bad-essids| filter-list]	Displays intrusion detection configuration parameters • configured-bad-essids – Displays a list of configured bad essids • filter-list – Displays the list of currently filtered mobile units
known *{ap statistics* {<1-1024>}}	Displays known AP parameters. • ap – Optional. Defines a known AP index <1-1024> • statistics – Optional. Displays known adaptive AP stats • <1-1024> – Optional. Displays adaptive ap statistics for known adaptive APs between 1-1024
mac-auth-local *{<1-1000>}*	Displays mac-auth-local entries for index <1-1000>.
mesh statistics *{<1-32>* {detail}}	Displays mesh related parameters • statistics – Displays mesh statistics • <1-32> – Optional. Defines the mesh index • detail – Optional Displays detailed mesh statistics

mobile-unit *{[<1-8192>|<MAC>|association-history| association-stats|probe-history|radio|roaming|statistics| voice|wlan]}*	Displays the parameters of associated mobile units. All parameters are optional. • <1-8192> – Index of mobile unit • <MAC> – MAC address of mobile unit • association-history *{<MAC>}*– Displays the association history of the Mobile Units with the MAC address and its configured name. • association-stats – Displays Statistics of associations and reassociations • probe-history [<1-200>|config-list] – Displays the probe history of the Mobile Unit with the address and its configured name • <1-200> – Defines index to display probe-logging • config-list – Lists probe history MAC addresses • radio <1-4096> – Displays the associated Mobile Units for the radio with the MAC address and its configured name. • RFS7000 supports <1-4096> radios • RFS6000 supports <1-1000> radios • roaming database – Displays the local mobile-unit roaming database. • statistics [<1-8192>|<MAC>|summary|voice] – Displays mobile unit RF statistics • <1-8192> – Displays Index of mobile-unit • <MAC> *{detail}*– Displays MAC address of mobile-unit. Optionally display detailed information. • summary – Displays RF-Stats summary of all currently associated mobile-units • voice [<1-4096>|<MAC>] – Displays mobile-unit voice statistics for a radio index or radio MAC address. • voice – Displays voice call details. • wlan <1-256> – Displays the MUs associated to the selected wlan

multicast-packet-limit	Displays the multicast-packet-limit
phrase-to-key [wep128|wep64] <pass-phrase>	Displays the WEP keys generated by a passphrase • wep128 – Displays WEP128 keys • wep64 – Displays WEP64 keys • <pass-phrase> – The passphrase to generate the keys for.
qos-mapping *{[wired-to-wireless| wireless-to-wired]}*	Quality of service mappings used for mapping WMM access categories and 802.1p/DSCP tags • wired-to-wireless – Mappings used when traffic is switched from the wired to the wireless side • wireless-to-wired – Mappings used when traffic is switched from the wireless to the wired side

radio *{[<1-4096>| admission-control|all| beacon-table|config| monitor-table|statistics| unadopted|uptime|voice] }*	Radio related commands. All parameters are optional. • <*1-4096*> – Defines information on a single radio's index • admission-control voice {<*1-4096*>} – Displays summary information for all radios that have admission control enabled. Optionally select the radio. • all – Displays information about all radios • beacon-table – Displays the radio-to-radio beacon table • config {[<*1-4096*>|default-11a|default-11an|default-11b| default-11bg|default-11bgn]} – Displays the selected radio's configuration. All parameters are optional. • <1-4096> – The radio index • default-11a – Default 11a configuration template • default-11an – Default 11an configuration template • default-11b – Default 11b configuration template • default-11bg – Default 11bg configuration template • default-11bgn – Default-11bgn configuration template • monitor-table – Displays the radio-to-radio monitoring table • statistics {[<1-4094>|long-interval|short-interval|voice]} – Displays a summary of radio statistics. All parameters are optional. • <1-4094> {detail} – Defines a single radio's index. Optionally display the details • long-interval – last 60 minutes for all adopted radios • short-interval – last 30 seconds for all adopted radios • voice {[<1-4096>|long-interval|short-interval]}– Displays voice related statistics for the selected option.

	• unadopted – Displays a list of unadopted radios • uptime – Displays the uptime of all adopted radios • voice <1-4094> – Displays voice call details • <1-4094> – Optional. Defines a single radio's index
radio-group *{<1-256>}*	Displays radios in specified group • <1-256> – Optional. A single radio index between < 1-256>. The index range varies based on the switch being used.
regulatory <country-code>	Regulatory (allowed channel/power) information for a particular country. • *<country-code>* – Two character country code for each country.
self-heal-config { [<1-4096>|all]}	Sets self healing configuration parameters • *<1-4096>* – Optional. Defines a single radio's index • all – Optional. Defines the self-healing configuration for all radios
sensor *{[<1-48>| default-config]}*	Defines *Wireless Intrusion Protection System* (WIPS) parameters • <1-48> – Specifies the index of a particular sensor to view detailed information about that sensor • default-config – Default configuration parameters for sensors

smart-rf [calibration-status| configuration| history|radio]	Displays smart-rf related management information • calibration-status – Displays smart-rf calibration status. • configuration – Displays smart-rf configuration information. • history – Displays smart-rf assignment history since last calibration. • radio [config|local-status|map|master-status|neighbors|spectrum] *{[<1-4096>|<MAC>| all-11a|all-11bg]}* – Displays smart-rf radio commands. • config – Displays the configuration information. • local-status – Displays the local radio status related to smart rf. • map – Maps all 11a radios in the configuration. • master-status – Displays the radio status from the master radio list. If no parameter is passed, displays status for all radios in the master list. • neighbors – Displays the radio's neighbor information • spectrum – Displays all 11a radios spectrum information <1-4096> – The selected radio • <MAC> – The selected radio MAC address • all-11a – All 11a radios • all-11bg – All 11bg radios
unapproved-aps	Defines unapproved APs seen by an access port or a mobile unit scan
wireless-switch-statistics *{detail}*	Displays wireless-switch statistics • detail – Optional Displays detailed wireless-switch statistics

wlan [config|statistics]	Displays wireless LAN parameters. The following information is displayed: • config [<1-256>|all|enabled] – Displays the wireless LAN configuration information. All parameters optional. • <1-256> – The selected wlan • all – all wlans in the configuration • enabled – all wlans that are enabled. Configuration information for disabled wlans are not displayed. • statistics <1-256> – Displays the wireless LAN statistics for: • <1-256> {detail} – The selected wlan. Optionally display details.

Example

```
RFSwitch>show wireless ap
Number of access-ports adopted  : 0
Available licenses        : 0
Clustering enabled        : N
Clustering mode         : primary
RFSwitch>

RFSwitch>show wireless ap-detection-config
Rogue  AP timeout   : 300 seconds
Approved AP timeout   : 300 seconds
mu-assisted scan     : enabled
mu-assisted scan refresh : 300 seconds
configured approved-aps :
Index | Bss Mac      | Ssid
-----------------------------------------------------
Adaptive minimum adoption version: 2.0.0.0-000R
RFSwitch>
RFSwitch>show wireless ap-images
 Idx  ap-type   Image-Name     Size (bytes) Version
  1  ap300   WISP-AP300       293516   00.02-29
  2  ap300   WIAP-300        244076   01.00-1635b
  3  ap300   AP300-IDS-Sensor    295064   00.00-04
  4  ap100   AP100          31034    02.05-00
  5  ap4131  AP4131         191440   07.00-01
  6  ap4131  Revert-AP4131      665704   00.00-00
```

```
RFSwitch>

RFSwitch>show wireless ap-unadopted
RFSwitch>

RFSwitch>show wireless approved-aps
access-port detection is disabled
RFSwitch>

RFSwitch>show wireless channel-power 11a indoor

RFSwitch>

RFSwitch(config)#show wireless config
country-code      : None
secure-wispe-default-secret default
adoption-pref-id    : 1
proxy-arp        : enabled
adopt-unconf-radio   : enabled
dot11-shared-key-auth  : disabled
ap-detection      : disabled
manual-wlan-mapping   : disabled
dhcp sniff state    : disabled
dhcp one portal forward : enabled
dhcp fix broadcast-rsp : disabled
broadcast-tx-speed   : optimize-for-range
wlan bw allocation   : disabled
smart-channels used   :
smart-channels excluded :
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited
user load balance mode : by-count
secure-wispe-default-secret : default
admission control for voice : enabled
cluster-master-support   : enabled
RFSwitch(config)#
```

```
RFSwitch>show wireless ids
 detect-window        : 10 seconds

 Excessive Operations:: Threshold(mu radio switch)  Filter-
Ageout
 probe-requests :      0   0   0       60 Sec
 association-requests :    0   0   0       60 Sec
 disassociations   :    0   0   0       60 Sec
 authentication-fails :    0   0   0       60 Sec
 crypto-replay-fails :    0   0   0       60 Sec
 80211-replay-fails  :    0   0   0       60 Sec
 decryption-fails   :    0   0   0       60 Sec
 unassoc-frames    :    0   0   0       60 Sec
 eap-starts      :    0   0   0       60 Sec


 Anomaly Detection::       Status   Filter-Ageout
 probe-requests      :  disabled   60 Sec
 association-requests   :  disabled   60 Sec
 disassociations     :  disabled   60 Sec
 authentication-fails   :  disabled   60 Sec
 crypto-replay-fails   :  disabled   60 Sec
 80211-replay-fails    :  disabled   60 Sec
 decryption-fails     :  disabled   60 Sec
 unassoc-frames      :  disabled   60 Sec
 eap-starts        :  disabled   60 Sec
 null-destination     :  disabled   60 Sec
 same-source-destination :  disabled   60 Sec
 multicast-source     :  disabled   60 Sec
 weak-wep-iv       :  disabled   60 Sec
 tkip-countermeasures   :  disabled   60 Sec
 invalid-frame-length   :  disabled   60 Sec
RFSwitch>

RFSwitch>show wireless mac-auth-local 50
RFSwitch>

RFSwitch>show wireless mobile-unit statistics

mobile-unit 1: <00-20-A6-52-5F-83>
WLAN : wlan-1
------ Traffic ----------------------------------------------
        Total Rx Tx

        30s 1hr 30s 1hr 30s 1hr
```

```
Pkts per sec:  1.73 0.00 0.87 0.00 0.87 0.00 pps
Throughput:   0.00 0.00 0.00 0.00 0.00 0.00 Mbps
Avg bit speed: 9.19 0.00 Mbps
% Non-unicast pkts: N/A N/A

------ RF Status----------------------------------------------

            30s 1hr
Avg mobile-unit signal: -78.00 0.00 dBm
Avg mobile-unit noise: -94.00 0.00 dBm
-- MORE --, next page: Space, next line: Enter, quit:
Control-C
Avg mobile-unit SNR(dB): 16.00 0.00

------ Errors-----------------------------------------------

            30s 1hr
Avg number of retries: 0.42 0.00
% gave up pkts: 0.00 0.00
% Non-decryptable pkts: 0.00 0.00


RFSwitch(config)#show wireless mobile-unit
index  MAC-address    radio type wlan vlan/tunnel ready IP-
address  last active Posture Status
 2   00-0E-9B-98-F9-34 1   11g 1   vlan 1  Y   192.168.2.45
0 Sec
Number of mobile-units associated: 1
RFSwitch(config)#



RFSwitch(config)#show wireless mobile-unit association-
history
MU MAC       Radio WLAN Timestamp     Event
============================================================
=
00-0E-9B-98-F9-34 1   1   1116316     Association
00-0E-9B-98-F9-34 1   1   12248923    Unassociation
00-0E-9B-98-F9-34 1   1   12250053    Association
00-0E-9B-98-F9-34 1   1   4280690527  Unassociation
00-0E-9B-98-F9-34 1   1   4280691647  Association
00-0E-9B-98-F9-34 1   1   4280716777  Unassociation
00-0E-9B-98-F9-34 1   1   4280717937  Association
RFSwitch(config)#
```

```
RFSwitch(config)#show wireless mobile-unit radio 1
index  MAC-address    radio type wlan vlan/tunnel ready IP-
address  last active Posture Status
 2   00-0E-9B-98-F9-34 1   11g 1   vlan 1  Y   192.168.2.45
0 Sec
Listed 1 of a total of 1 mobile-units
RFSwitch(config)#

RFSwitch(config)#show wireless wlan config 1
WLAN: 1, status: enabled, description: WLAN1, ssid:
sardarjee
 auth: none, encr: none, inactivity-timeout: 1800 seconds
 vlan 1: unlimited users
 mu-mu-disallow: disabled, secure-beacon: disabled, answer-
bcast-ess: enabled,
 weight: 1, prioritize-voice: disabled, spectralink-voice-
protocol: disabled
 multicast mask1: 00-00-00-00-00-00, mask2: 00-00-00-00-00-
00
 traffic-classification : normal, wmm-mapping: 8021p, L3-
mobility: disabled
 Client Bridge Backhaul is disabled on this WLAN
 NAC Mode: bypass-nac-except-include-list

Exclude list(s): NotMe
RFSwitch(config)#
```

2.2.37 wlan-acl

- *Common to all modes*

Displays the WLAN based access control list information

Syntax

```
show wlan-acl [<1-256>|all]
```

Parameters

wlan-acl [<1-256>|all]	Displays WLAN based access control list information • <1-256> – Displays ACLs attached to the specified WLAN ID • all – Displays all ACLs attached to a WLAN port

Example

```
RFSwitch>show wlan-acl 20
WLAN port: 20
 Inbound IP Access List  :
 Inbound MAC Access List :
 Outbound IP Access List :
 Outbound MAC Access List :
RFSwitch>

RFSwitch>show wlan-acl all
WLAN port: 1
 Inbound IP Access List  :78
 Inbound MAC Access List :200
 Outbound IP Access List :78
 Outbound MAC Access List :200
RFSwitch>
```

2.2.38 access-list

▸ *Privilege / Global Config*

Displays the access lists (numbered and named) configured on the switch. The numbered access list displays numbered ACLs. The named access list displays named ACL details.

Syntax

```
show access-list [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<acl-name>]
```

Parameters

access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>]	Displays access-list entries. • <1-99> - IP standard access list • <100-199> - IP extended access list • <1300-1999> - IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <acl-name> - Name of ACL

Example

```
RFSwitch(config)#show access-list
Extended IP access list 110
  permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence
5
  permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence
63
  permit ip 192.168.157.0/24 192.168.100.0/24 rule-
precedence 157
RFSwitch(config)#

RFSwitch(config)#show access-list 110
Extended IP access list 110
  permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence
5
  permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence
63
  permit ip 192.168.157.0/24 192.168.100.0/24 rule-
precedence 157
RFSwitch(config)#
```

2.2.39 aclstats

▸ *Privilege / Global Config*

Displays the statistics of configured access lists

Syntax

```
aclstats [access-list|vlan <1-4094>]
aclstats {<1-99>|<100-199>|<1300-1999>|<2000-2699>|
<acl-name>}
aclstats vlan <1-4094>
```

Parameters

access-list {<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>}	Displays configured access lists. • <1-99> - IP standard access list • <100-199> - IP extended access list • <1300-1999> - IP standard access list (expanded range) • <2000-2699> - IP extended access list (expanded range) • <acl-name> - Name of ACL
vlan <1-4094>	Defines the VLAN interface (between 1- 4094)

Example

```
RFSwitch(config)#show vlan 400
RFSwitch(config)#
```

2.2.40 alarm-log

▸ *Privilege / Global Config*

Displays the contents of the alarm log on the device

Syntax

```
show alarm-log {<1-65535>|acknowledged|all|count|new|
severity-to-limit}
show alarm-log severity-to-limit {critical|
 informational|major|normal|warning}
```

Parameters

alarm-log [<1-65535>| acknowledged|all|count| new| severity-to-limit]	Displays the contents of the alarm log on the device. • <1-65535> - Displays the details of a specific alarm ID • acknowledged - Displays information for acknowledged alarms currently in the system • all - Displays all the alarms currently in the system • count - Displays the number (count) of the alarms currently in the system • new - Displays those new alarms currently in the system • severity-to-limit {critical|informational major|normal|warning} - Displays the alarms having specified severity, as well as those alarms with a severity higher than the specified value. • critical - Displays all critical alarms • informational - Displays all informational or higher severity alarms • major - Displays all major or higher severity alarms • normal - Displays all normal or higher severity alarms • warning - Displays all warning or higher severity alarms

2.2.41 boot

Privilege / Global Config

Displays the boot configuration of the device

Syntax

```
show boot
```

Parameters

None

Example

```
RFSwitch#show boot

Image      Build Date       Install Date      Version
-----    -------------------  -------------------   ------
--------
Primary   Oct 16 03:55:43 2008   Sep 15 00:53:56 2008
1.3.0.0-018B
Secondary  Sep 30 00:14:30 2008   Aug 27 01:46:32 2008
1.3.0.0-015B

Current Boot    : Primary
Next Boot     : Primary
Software Fallback : EnabledRFSwitch#
```

2.2.42 clock

- *Privilege / Global Config*

Displays the system clock

Syntax

```
show clock
```

Parameters

None

Example

```
RFSwitch#show clock
Jun 01 00:51:34 UTC 2007
RFSwitch#
```

2.2.43 debugging

- *Privilege / Global Config*

Displays the debugging configuration information

Syntax

```
show debugging mstp
```

Parameters

mstp	Displays the current MSTP configuration

Example

```
RFSwitch(config)#show debugging mstp
MSTP debugging status:
RFSwitch(config)#
```

2.2.44 dhcp

- *Privilege / Global Config*

Displays existing DHCP server configurations

Syntax

```
show dhcp [config|status]
```

Parameters

config	Displays the current DHCP server configuration
status	Displays whether the DHCP server is running

Example

```
RFSwitch#show dhcp config

service dhcp
!
ip dhcp pool vlan6
 default-router xxx.xxx.xxx.2
 network xxx.xxx.xx.0/24
 address range xxx.xxx.xx.xx aaa.aaa.aa.aa

RFSwitch#
```

2.2.45 file

Privilege / Global Config

Displays the filesystem information

Syntax

```
show file [information|systems]
```

Parameters

file [information|systems]	Displays the filesystem information. • information <FILE> - Displays file information • <FILE> - Displays the information on file • systems - Lists existing filesystems

Example

```
RFSwitch#show file systems
File Systems:

   Size(b)   Free(b)   Type Prefix
      -         -   opaque system:
  13704192  11904000  flash nvram:
  19524608  16866304  flash flash:
      -         - network sftp:
      -         - network http:
      -         - network ftp:
      -         - network tftp:
RFSwitch#
```

2.2.46 ftp

- *Privilege / Global Config*

Displays the FTP server configuration

Syntax

```
show ftp
```

Parameters

None

Example

```
RFSwitch#show ftp
FTP Server: Disabled
User Name: anonymous or ftpuser
Password:  ********
Root dir:  flash:/
RFSwitch#
```

2.2.47 password-encryption

Privilege / Global Config

Displays the global password encryption status

Syntax

```
show password-encryption status
```

Parameters

status	Displays the existing password-encryption status

Example

```
RFSwitch#show password-encryption status
Password encryption is disabled
RFSwitch#
```

2.2.48 running-config

▸ *Privilege / Global Config*

Displays the contents of those configuration files wherein all configured MAC and IP access lists are applied to an interface

Syntax

```
show running-config [full|include-factory]
```

Parameters

running-config [full|include-factory]	Displays the contents of the configuration files • full – Displays the file's full (complete) configuration • include-factory – Includes factory defaults

Example

```
RFSwitch(config)#show running-config
!
! configuration of RFSwitch version 4.0.0.0-008D
!
version 1.0
!
service prompt crash-info
!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst config
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server sysname RFSwitch
snmp-server manager v2
snmp-server manager v3
```

```
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
fallback enable
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 wlan 1 enable
 wlan 1 ssid sardarjee
 radio add 1 00-A0-F8-BF-8A-4B 11bg ap300
 radio add 2 00-A0-F8-BF-8A-4B 11a ap300
 enhanced-beacon-table enable
 enhanced-beacon-table channel-set a 36 44 149
 enhanced-beacon-table channel-set bg 1 2 4 5
!
radius-server local
!
interface eth1
 switchport access vlan 2100
!
interface eth2
 switchport access vlan 1
!
interface vlan1
 ip address 192.168.2.1/24
!
sole
!
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end
```

```
RFSwitch(config)#

RFSwitch(config)#show running-config include-factory
!
! configuration of RFSwitch version 4.0.0.0-008D
!
version 1.0
!
service prompt crash-info
no service set command-history
no service set reboot-history
no service set upgrade-history
!
hostname RFSwitch
!
banner motd Welcome to CLI!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin access console web ssh telnet
username admin privilege superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username operator access console web ssh telnet
username operator privilege monitor
!
!
!
!
spanning-tree mst config
 name My Name
!
no management secure
ip domain-lookup
service diag period 1000
service diag enable
country-code us
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
redundancy hold-period 15
redundancy heartbeat-period 5
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy dhcp-server enable
no redundancy enable
```

```
.................................................
.................................................
.................................................
.................................................
no radio default-11b enhanced-beacon-table
no radio default-11b enhanced-probe-table
no radio 1 neighbor-smart-scan
no radio 2 neighbor-smart-scan
no ap-detection enable
.................................................
.................................................
.................................................
.................................................
ip address 123.111.2.1/24
 no ip helper-address
!
sole
 no adapter AeroScout enable
!
radius-server retransmit 3
radius-server timeout 5
radius-server key
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

RFSwitch(config)#
```

2.2.49 securitymgr

▸ *Privilege / Global Config*

Displays the security manager event-logs

Syntax

```
show securitymgr event-logs
```

Parameters

None

Example

```
RFSwitch#show securitymgr event-log
RFSwitch#
```

2.2.50 sessions

- *Privilege / Global Config*

Displays the list of current active open sessions on the device

Syntax

```
show sessions
```

Parameters

None

Example

```
RFSwitch#show sessions
SESSION  USER    LOCATION    IDLE     START TIME
  1    cli  Console      06:24m   May 31 18:31:36 2007
** 2    cli  10.10.10.1    00:00m   Jun 1 00:04:30 2007
RFSwitch#
```

2.2.51 startup-config

Privilege / Global Config

Displays the complete startup configuration script on the console

Syntax

```
show startup-config
```

Parameters

None

Example

```
RFSwitch#show startup-config
!
! configuration of RFSwitch version 4.0.0.0-008D
!
version 1.0
!
service prompt crash-info
!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst config
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server sysname RFSwitch
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
```

```
fallback enable
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 wlan 1 enable
 wlan 1 ssid sardarjee
 radio add 1 00-A0-F8-BF-8A-4B 11bg ap300
 radio 1 enhanced-beacon-table
 radio 1 enhanced-probe-table
 radio add 2 00-A0-F8-BF-8A-4B 11a ap300
 ap-detection approved add 1 any any
 enhanced-beacon-table enable
 enhanced-beacon-table channel-set a 36 44 149
 enhanced-beacon-table channel-set bg 1 2 4 5
!
radius-server local
!
interface eth1
 switchport access vlan 2100
!
interface eth2
 switchport access vlan 1
!
interface vlan1
 ip address 192.168.2.1/24
!
sole
!
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

RFSwitch#
```

2.2.52 upgrade-status

▸ *Privilege / Global Config*

Displays the last image-upgrade status

Syntax

```
show upgrade-status {detail}
```

Parameters

None

Example

```
RFSwitch#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time  : Mon May 21 16:27:40 2007
RFSwitch#
```

2.2.53 mac-name

- *User Exec*

Displays the configured MAC name

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show mac-name
```

Parameters

None

Example

```
RFSwitch(config-wireless)#show mac-name
Index  MAC Address    MAC Name
 1   00-18-DE-82-78-6B GE1PortMACAddress
Number of MAC names configured = 1
RFSwitch(config-wireless)#
```

2.2.54 access-list

▸ *Priv Exec*

Displays the access control list entries based on the ACL name or index

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show access-list {<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<acl-name>}
```

Parameters

access-list {<1-99>| <100-199>|<1300-1999>| <2000-2699>|<acl-name>}	Displays ACL entry details. • <1-99> – Lists the IP standard access-list entries • <100-199> – Lists the IP extended access-list entries • <1300-1999> – Lists the IP standard access-list (expanded range) entries • <2000-2699> – Lists the IP extended access-list (expanded range) entries • <acl-name> – Lists the entry specified by the ACL name <acl-name>

Example

```
RFSwitch#show access-list 1
Standard IP access list 1
  permit host 192.168.10.1 rule-precedence 10
RFSwitch#
```

2.2.55 aclstats

Displays the ACL statistics for the selected vlan

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show aclstats [access-list|vlan]
show aclstats access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>]
show aclstats vlan <1-4094>
```

Parameters

aclstats [access-list|vlan]	Displays the ACL statistics. • access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|<acl-name>] – Displays the access control list entries based on their index • <1-99> – Lists the IP standard access-list entries • <100-199> – Lists the IP extended access-list entries • <1300-1999> – Lists the IP standard access-list (expanded range) entries • <2000-2699> – Lists the IP extended access-list (expanded range) entries • <acl-name> – Lists the entry specified by the ACL name <acl-name> • vlan <1-4094> – Selects the interface for which to display ACL statistics.

Example

```
RFSwitch#show aclstats vlan 10
RFSwitch#
```

2.2.56 alarm-log

▸ *Priv Exec Mode*

Displays all the alarms on the system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show alarm-log {<1-65535>|acknowledged|all|count|new|
  severity-to-limit}
```

Parameters

alarm-log [<1-65535>| acknowledged|all|count| new| severity-to-limit]	Displays all the alarms on the system • <1-65535> - Displays the details of a specific alarm ID • acknowledged - Displays information for acknowledged alarms currently in the system • all - Displays all the alarms currently in the system • count - Displays the number (count) of the alarms currently in the system • new - Displays those new alarms currently in the system • severity-to-limit [critical|informational major|normal|warning] - Displays the alarms having specified severity, as well as those alarms with a severity higher than the specified value. • critical - Displays all critical alarms • informational - Displays all informational or higher severity alarms • major - Displays all major or higher severity alarms • normal - Displays all normal or higher severity alarms • warning - Displays all warning or higher severity alarms

Example

```
RFSwitch#show alarm-log 1
RFSwitch#

RFSwitch#show alarm-log acknowledged
RFSwitch#

RFSwitch#show alarm-log severity-to-limit
```

2.2.57 firewall

Priv Exe Mode

Displays wireless firewall

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show firewall [config|flow]
show firewall [config|flow timeouts]
```

Parameters

firewall [config| flow timeouts]	Displays firewall configuration information. • config – Displays Configuration • flow timeouts – Displays firewall flow • timeouts - Flow timeout configuration

Example

```
RFSwitch#show firewall
RFSwitch#

RFSwitch#show firewall config
RFSwitch#

RFSwitch#show firewall flow
RFSwitch#
```



NOTE: For information on the 'firewall' command in Global Config mode, refer to *firewall on page 5-124*.

2.2.58 role

▸ *Priv Exe Mode*

Displays existing role name

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
show role [<role-name>|mobile-units]
```

Parameters

role [<role-name>| mobile-units]	Displays existing role name • <role-name> – Displays existing role name • mobile-units – Displays mobile-units assigned with these roles

Example

```
RFSwitch#show role
RFSwitch#

RFSwitch#show role word
RFSwitch#

RFSwitch#show role mobile-units
RFSwitch#
```

3

User Exec Commands

Logging in to the switch places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before a connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use **?** at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (**>**). The default host name is generally "WLAN Module". Use the GLOBAL CONFIG command to change the hostname.

3.1 User Exec Commands

Table 3.1 summarizes USER EXEC commands:

Table 3.1 User Exec Mode Command Summary

Command	Description	Ref.
clear	Resets the command to the previous configuration	*page 3-3*
clrscr	Clears the display screen	*page 2-2*
cluster-cli	Displays the cluster context	*page 3-5*
debug	Displays debugging functions	*page 3-6*
disable	Turns off (disables) the privileged mode command set	*page 3-8*

Table 3.1 User Exec Mode Command Summary

Command	Description	Ref.
enable	Turns on (enables) the privileged mode command set	*page 3-9*
exit	Ends the current mode and moves down to the previous mode	*page 2-3*
help	Describes the interactive help system	*page 2-4*
logout	Exits the EXEC mode	*page 3-10*
no	Negates a command or sets its defaults	*page 2-5*
page	Toggles the paging functionality	*page 3-11*
ping	Sends ICMP echo messages	*page 3-12*
quit	Exits the current mode and moves to the previous mode	*page 3-13*
service	Displays service commands	*page 2-7*
show	Shows running system information. Refer to *Common Commands on page 2-1*	*page 2-37*
telnet	Opens a telnet session	*page 3-14*
terminal	Sets terminal line parameters	*page 3-15*
traceroute	Traces the route to a destination	*page 3-16*

3.1.1 clear

User Exec Commands

Resets the previous (last saved) command

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: Refer to the interface details below when using `clear counter interface`.

- ge <1-4> – Available only in RFS7000
- ge <1-8> – Available only in RFS6000
- me1 – Available in both RFS7000 and RFS6000
- up1 – Available only in RFS6000
- sa <1-4> – Available only in RFS7000

Syntax

```
clear [crypto|mobility|spanning-tree]

clear crypto [ipsec|isakmp] sa {<IP>}

clear mobility [event-log|mobile-unit|peer-statistics]
clear mobility event-log [mobile-unit|peer]
clear mobility mobile-unit [<MAC>|all|foreign-database|
  home-database]
clear mobility peer-statistics {<Peer-IP>}

clear spanning-tree detected-protocols {interface
<interface-name>}
```

Parameters

crypto [ipsec|isakmp] sa *{<IP>}*	Clears IPSec/ISAKMP SAs for a given peer • ipsec sa *{<IP> }* – Clears IPSec SA's • isakmp sa *{<IP> }* – Clears ISAKMP SA's • sa – Clears all IPSec/ISAKMP SA's • <IP> – Optional. Peer IP address

mobility [event-log| mobile-unit| peer-statistics]	Clears mobility attributes • event-log [mobile-unit|peer]– Clears the event log • mobile-unit – Clears MU event-logs for • peer – Clears peer event logs • mobile-unit [<MAC>|all|foreign-database| home-database] – Clears MU information. • <MAC> – Clears the MAC addresses of a MU • all – Clears the MU MAC address, including the foreign and home database • foreign-database – Clears those MUs present in the foreign MU database • home-database – Clears those MUs present in the home MU database • peer-statistics {<Peer-IP>} – Clears Mobility Peer Statistics • <Peer-IP> – Optional. IP address of a Peer
spanning-tree detected-protocols *{interface <interface-name>}*	Clears the spanning tree protocols configured for the interface • detected-protocols *{interface <interface-name>}* – Enter the optional interface name <interface-name> to clear the detected spanning tree protocols for that specific interface

Example

```
RFSwitch>clear crypto ike sa 111.222.333.01
RFSwitch>
```

3.1.2 cluster-cli

User Exec Commands

Use this command to enter the cluster-cli context. The cluster-cli context provides centralized management to configure all cluster members from any one member. Any command executed under this context will be executed to all the switches in the cluster.

A new context *redundancy* supports the cluster-cli. Any commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the cluster context

Example

```
RFSwitch> enable
RFSwitch:cluster-cli>
```

3.1.3 debug

User Exec Commands

Use this command to debug the switch

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
debug [certmgr|ip|mobility]
debug certmgr [all|error|info]
debug ip [https|ssh]
debug mobility [cc|error|forwarding|mu|packet|peer|system]
debug mobility forwarding {<MAC>}
```

Parameters

certmgr [all|error|info]	Certificate Manager Debugging Messages • all – Traces error and informational messages from the certificate manager • error – Traces error messages from the certificate manager. • info – Traces informational messages from the certificate manager
ip [https|ssh]	Internet Protocol (IP) debug messages • https – Secure HTTP (HTTPS) server • ssh – Secured Shell (SSH) server

mobility [cc|error|forwarding|mu| packet|peer|system]	L3 mobility debug messages. • cc – ccserver events • error – Error events • forwarding <MAC> – Dataplane forwarding • <MAC> – MAC Address of the station • mu – MU events and state changes • packet – Control packets events • peer – Peer establishments • system – System events

Examples

```
RFSwitch>debug certmgr all
RFSwitch>debug certmgr info
RFSwitch>debug ip ssh
RFSwitch>debug mobility cc
RFSwitch>debug mobility error
RFSwitch>debug mobility forwarding
RFSwitch>debug mobility mu
RFSwitch>debug mobility packet
RFSwitch>debug mobility peer
RFSwitch>debug mobility system
RFSwitch>
```

3.1.4 disable

User Exec Commands

Enables the PRIV mode to use the disable command. Use the `disable` command to exit the PRIV mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`disable`

Parameters

None

Example

```
RFSwitch>disable
RFSwitch>
```

3.1.5 enable

User Exec Commands

Use the enable command to enter the PRIV mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
enable
```

Parameters

None

Example

```
RFSwitch>enable
RFSwitch#
```

3.1.6 logout

User Exec Commands

Use this command instead of the `exit` command to exit the EXEC mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`logout`

Parameters

None

Example

```
The RFSwitch Series Switch logs off on execution of this
command.
```

3.1.7 page

User Exec Commands

Use the command to toggle the switch paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

page

Parameters

None

3.1.8 ping

User Exec Commands

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`ping {[<IP>|<hostname>]}`

Parameters

ping *{[<IP>|<hostname>]}*	Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts you for an IP/Host-name to ping.

Example

```
RFSwitch>ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100): 100 data bytes
128 bytes from 192.168.2.100: icmp_seq=0 ttl=128 time=2.7 ms
128 bytes from 192.168.2.100: icmp_seq=1 ttl=128 time=38.4
ms
128 bytes from 192.168.2.100: icmp_seq=2 ttl=128 time=4.6 ms

--- 192.168.2.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.7/15.2/38.4 ms
RFSwitch>ping
Target IP address:
```

3.1.9 quit

User Exec Commands

Use this command to exit the current mode and move to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`quit`

Parameters

None

Example

The switch logs off upon execution of the command

3.1.10 telnet

User Exec Commands

Opens a telnet session

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
telnet <IP> port
```

Parameters

telnet <IP> port	Defines the IP address or hostname of a remote system • port – Displays TCP port number

Example

```
RFS7000>telnet 172.16.10.3

Entering character mode
Escape character is '^]'.


RFS6000 release 4.0.0.0-037D
Login as 'cli' to access CLI.
RFS6000 login:
```

3.1.11 terminal

User Exec Commands

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
terminal [length <0-512>|no [length <0-512>|width]|
  width <0-512>]
```

Parameters

length <0-512>	Sets the number of lines on a screen
no [length <0-512>| width]	Negates a command or sets its defaults. • length <0-512> – Negates the length command • width – Negates the width command
width <0-512>	Sets the width/number of characters on a screen line

Example

```
RFSwitch>terminal length 100
RFSwitch>

RFSwitch>terminal width 200
RFSwitch>
```

3.1.12 traceroute

User Exec Commands

Traces the route to its defined destination

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
traceroute [[<IP>|<hostname>]|ip [<IP>|<hostname>]]
```

Parameters

[<IP>|<hostname>]	Traces the route to a destination IP address or a hostname
ip [<IP>|<hostname>]	IP trace to a destination IP address or a hostname

Example

```
RFSwitch#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max,
38 byte packets
1 157.235.208.39 (157.235.208.39) 0.466 ms 0.363 ms 0.226 ms
RFSwitch#
```

4

Privileged Exec Commands

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (**#**). To access the PRIV EXEC mode, enter the following at the prompt:

```
RFSwitch>enable
RFSwitch#
```

The PRIV EXEC mode is often referred to as the *enable mode*, because the `enable` command is used to enter the mode. There is no provision to configure a password to get access to PRIV EXEC (enable) mode.

4.1 Priv Exec Command

Table 4.1 summarizes the switch PRIV EXEC commands:.

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
acknowledge	Acknowledges alarms	*page 4-4*
archive	Manages archive files	*page 4-5*
cd	Changes the current directory	*page 4-7*
change-passwd	Changes the password of the logged user	*page 4-8*

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
clear	Resets switch functions to last saved configuration	*page 4-9*
clock	Configures the software system clock	*page 4-13*
clrscr	Clears the displayed screen	*page 2-2*
cluster-cli	Displays the cluster context	*page 4-14*
configure	Enters the configuration mode	*page 4-15*
copy	Copies content from one file to another	*page 4-16*
debug	Displays debugging functions	*page 4-17*
delete	Deletes a specified file from the system	*page 4-25*
diff	Displays differences between two files	*page 4-26*
dir	Lists the files on a filesystem	*page 4-28*
disable	Turns off privileged mode command	*page 4-29*
edit	Edits a text file	*page 4-30*
enable	Turns on the privileged mode command	*page 4-31*
erase	Erases a filesystem	*page 4-32*
exit	Ends the current mode and moves to the previous mode	*page 2-3*
halt	Halts the switch	*page 4-33*
help	Displays a description of the interactive help system	*page 2-4*
kill	Kills (terminates) a specified session	*page 4-34*
logout	Exits the EXEC mode	*page 4-35*
mkdir	Creates a directory	*page 4-36*
more	Displays the contents of a file	*page 4-37*

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
no	Negates a command or sets its defaults	*page 2-5*
page	Toggles the paging function	*page 4-39*
ping	Sends ICMP echo messages to a specified location	*page 4-40*
pwd	Displays the current directory	*page 4-41*
quit	Exits the current mode and moves to the previous mode	*page 4-42*
reload	Halts the switch and performs a warm reboot	*page 4-43*
rename	Renames a file	*page 4-44*
rmdir	Deletes a directory	*page 4-45*
service	Displays service commands	*page 2-7*
show	Shows running system information.	*page 2-37*
telnet	Opens a telnet session	*page 4-46*
terminal	Sets terminal line parameters	*page 4-47*
traceroute	Traces a route to a destination	*page 4-48*
upgrade	Upgrades the switch software image	*page 4-49*
upgrade - abort	Aborts an ongoing upgrade operation	*page 4-51*
write	Writes the running configuration to memory or a terminal	*page 4-52*

4.1.1 acknowledge

Priv Exec Command

Acknowledges alarms

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
acknowledge alarm-log [<1-65535>|all]
```

Parameters

alarm-log [<1-65535>|all]	Acknowledges alarms • <1-65535> – Acknowledges the specific alarm ID • all – Acknowledges all alarms

Example

```
RFSwitch#acknowledge alarm-log all
No corresponding record found in the Alarm Log.

RFSwitch#acknowledge alarm-log 200
No corresponding record found in the Alarm Log.
RFSwitch#
```

4.1.2 archive

Priv Exec Command

Manages file archive operations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] [<FILE>|<DIR>]
archive tar /xtract [<FILE>|<URL>] <DIR>
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file
/table	Lists the files in a tar file
/create	Creates a tar file
/xtract	Extracts content from a tar file
<FILE>	Defines a Tar filename
<URL>	Tar file URL
<DIR>	A directory name. When used with /create, is the source directory for the tar file. When used with /xtract, is the destination file where the contents of the tar file are extracted to.

Example

How to zip the folder flash:/log/?

```
RFSwitch#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
```

```
RFSwitch#dir flash:/
```

How to view the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Apr 17 08:25:50 2007   hotspot
  drwx   120       Fri Apr  8 12:27:20 2007   log
  drwx   1024      Thu Apr  7 16:23:34 2007   crashinfo
  drwx   1024      Wed May 23 15:30:19 2007   backup
  -rw-   173056    Fri May  8 14:39:48 2007   out.tar
```

How to see which files are in the tar file?

```
RFSwitch#archive tar /table flash:/out.tar
drwxrwxrwt 0/600  0 2007-05-08 12:27:20 flash/log
-rw-r--r-- 0/0    381 2007-05-08 12:27:28 flash/log/
snmpd.log
-rw-r--r-- 0/0    151327 2007-05-08 14:37:26 flash/log/
messages.log
-rw-r--r-- 0/0    17318 2007-05-08 12:27:29 flash/log/
startup.log
drwxrwxrwt 0/600  0 2007-05-08 12:27:14 flash/log/radius
```

If Untar fails..?

```
RFSwitch#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

4.1.3 cd

Priv Exec Command

Changes the current directory

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`cd {<DIR>}`

Parameters

<DIR>	Changes current directory to DIR. This parameter is optional. When this parameter is not provided, the current directory name is displayed.

Example

```
RFSwitch#cd
nvram:/   system:/  flash:/

RFSwitch#cd flash:/?
  DIR  Change current directory to DIR

RFSwitch#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/
flash:/log/
flash:/out/

RFSwitch#cd flash:/log/?
  DIR  Change current directory to DIR

RFSwitch#cd flash:/log/
RFSwitch#pwd
flash:/log/
RFSwitch#
```

4.1.4 change-passwd

Priv Exec Command

Changes the password of a logged user

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`change-passwd`

Parameters

None

Usage Guidelines

A password must be between 8 to 32 characters in length. For security, the console does not display user entered key words or the old password and new password fields.

Verify the console displays a "password successfully changed" message.



NOTE: The console (by default), does not display a user entered keyword for an old password and new password.

Leaving the old password and new password fields empty displays the following error message:
`Error: Invalid password length. It should be between 8 - 32characters.`

Example

```
RFSwitch#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
RFSwitch#
```

4.1.5 clear

Priv Exec Command

Resets the current context

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clear [aclstats|alarm-log|arp-cache|counters|crypto|
  dosstats|ip|logging|mac-address-table|mobility|
  spanning-tree]
clear [aclstats|arp-cache|dosstats|logging]

clear alarm-log [<1-65535>|acknowledge|all|new]

clear counters [all|bridge|firewall|igmp-snooping|interface|
  router|thread]
clear counters interface [<interface>|all|ge <1-8>|me1|sa
<1-4>|up1|vlan <1-4094>]

clear crypto [ike|ipsec] sa {<IP>}

clear ip [dhcp|pmtu-discovery-blackhole-cache]
clear ip dhcp binding [*|<IP>|all]
clear ip pmtu-discovery-blackhole-cache

clear mac-address-table [dynamic|multicast|static]
  [address <address>|bridge <1-32>|interface <interface>|
  vlan <vlan>]

clear mobility [event-log|mobile-unit|peer-statistics]
clear mobility event-log [mobile-unit|peer]
clear mobility mobile-unit [<MAC>|all|foreign-database|
  home-database]
clear mobility peer-statistics {<peer-IP>}

clear spanning-tree detected-protocols {interface
<interface-name>}
```

Parameters

aclstats	Clears ACI statistics

alarm-log [<1-65535>| acknowledge|all|new]	Clears the alarm-log • <1-65535> – Clears the specific alarm ID • acknowledge – Clears acknowledged alarms • all – Clear all alarms • new – Clear new alarms
arp-cache	Clears the ARP cache
counters [all|bridge|firewall| igmp-snooping|interface| router|thread]	Clears counters • all – Clears all counters • bridge – Clears bridge counters • firewall – Clears firewall counters • interface [<interface>|all|ge <1-8>|me1|sa <1-4>|up1| vlan <1-4094>] – Clears interface counters • igmp-snooping – Clears igmp-snooping counters • router – Clears router counters • thread – Clear per-thread counters
crypto [ipsec|isakmp] sa *{<IP>}*	Clears IPSec/ISAKMP SAs for a given peer • ipsec sa {<IP> } – Clears IPSec SA's • isakmp sa {<IP> } – Clears ISAKMP SA's • sa – Clears all IPSec/ISAKMP SA's • <IP> – Optional. Peer IP address
ip [dhcp| pmtu-discovery-blackhole-cache]	Clears Internet Protocol (IP) DHCP/NAT • dhcp binding [*|<IP>|all]– DHCP server configuration • binding [*|<IP>|all]– DHCP address bindings • * – Clears all bindings • <IP> – Clears a specific IP binding • all – Clears • pmtu-discovery-blackhole-cache - Clears path For more details, see *DHCP Server Instance on page 17-1*
logging	Modifies message logging facilities

mac-address-table [dynamic|multicast|static] [address <address>| bridge <1-32>| interface <interface>| vlan <vlan>]	Clears entries in the forwarding database • dynamic – Clears all dynamic entries • multicast – Clears all multicast entries • static – Clears all management configured entries • address <address> – Clears a specified MAC address • bridge <1-32> – Clears bridge group commands • interface <interface> – Clears all MAC addresses for the specified interface • vlan <vlan> – Clears all MAD addresses for the specified VLAN (1-4094)
mobility [event-log| mobile-unit| peer-statistics]	Clears mobility attributes • event-log [mobile-unit|peer]– Clears the event log • mobile-unit – Clears MU event-logs for • peer – Clears peer event logs • mobile-unit [<MAC>|all|foreign-database home-database] – Clears MU information. • <MAC> – Clears the MAC addresses of a MU • all – Clears the MU MAC address, including the foreign and home database • foreign-database – Clears those MUs present in the foreign MU database • home-database – Clears those MUs present in the home MU database • peer-statistics {<peer-IP>}– Clears Mobility Peer Statistics • <peer-IP> – IP address of a Peer
spanning-tree detected-protocols *{interface <interface-name>}*	Clears the spanning tree protocols configured for the interface • detected-protocols *{interface <interface-name>}* – Enter the optional interface name to clear the detected spanning tree protocols for that specific interface

Example

```
RFSwitch#clear alarm-log new
RFSwitch#
RFSwitch#clear alarm-log acknowledged
RFSwitch#
RFSwitch#clear arp-cache
RFSwitch#
RFSwitch#clear logging
RFSwitch#
RFSwitch#clear mobility event-log peer
RFSwitch#
RFSwitch#clear ip dhcp binding *
RFSwitch#
```

4.1.6 clock

Priv Exec Command

Configures the software system clock

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clock set HH:MM:SS <1-31> <MONTH> <1993-2035>
```

Parameters

HH:MM:SS	Sets the time in hours, minutes, and seconds
<1-31>	Sets the number of days in the month.
<MONTH>	Sets the month in the format Jan, Feb, Mar,..., Dec.
<1993-2035>	Sets the year

Example

```
RFSwitch#clock set 15:10:30 25 May 2007

RFSwitch#show clock
May 25 15:10:31 UTC 2007
```

4.1.7 cluster-cli

Priv Exec Command

Use this command to access the cluster-cli context. The cluster-cli context provides centralized management to configure all members of cluster from one member. Any command executed under this context is executed on all switches in the cluster.

A new context (*redundancy*) is available to support the cluster-cli. Any commands executed under this context are executed on each cluster member.

Use `no cluster-cli` to exit the cluster-cli context.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the switch cluster context

Example

```
RFSwitch#cluster-cli enable
```

4.1.8 configure

Priv Exec Command

Enters the configuration mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
configure terminal
```

Parameters

terminal	Enables configuration from the terminal

Example

```
RFSwitch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFSwitch(config)#
```

4.1.9 copy

Priv Exec Command

Copies any file (config,log,txt ...etc) from any location to the switch and vice-versa



NOTE: Copying a new config file onto an existing running-config file merges it with the existing running-config on the switch. Both, the existing running-config and the new config file are applied as the current running-config.

Copying a new config file onto a start-up config files replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
copy [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

<FILE>	The first <FILE> is the source file to copy from. The second <FILE> is the destination to which to copy.
<URL>	The first <URL> is the source URL to copy from. The second <URL> is the destination URL to which to copy.

Example

Transferring file snmpd.log to remote tftp server?

```
RFSwitch#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
RFSwitch#copy tftp://157.235.208.105:/running-
config running-config
```

4.1.10 debug

Priv Exec Command

Use this command for debugging

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
debug [all|cc|ccstats|certmgr|dhcpsvr|imi|ip|logging|mgmt|
  mobility|mstp|nsm|radius|redundancy|rns|securitymgr|sole]
debug all
debug cc [access-port|all|alt|ap-containment|ap-detect|
  capwap|cluster|config|dot11|eap|ids|kerberos|l3-mob|
  loc-ap|loc-mu|media|mobile-unit|radio|radius|self-heal|
  smart|snmp|system|wips|wisp|wlan] {[debug|err|info|warn]}

debug ccstats <statsmodule>
debug [certmgr|dhcpsvr] [all|error|info]
debug imi [all|cli-client|cli-server|errors|init|ntp]
debug ip [https|ssh]
debug logging [all|errors|init|monitor|subagent]
debug mgmt [all|debug|err|info|sys|warning]
debug mobility [all|cc|error|forwarding|mu|packet|peer|
  system]
debug mstp [all|cli|packet|protocol|timer]
debug nsm {[all|events|kernel|packet]}
debug radius {[all|err|info|warn]}
debug redundancy [all|ccmsg|config|errors|general|
  heartbeats|init|packets|proc|shutdown|states|subagent|
  timer|warnings]
debug securitymgr [acldebug|aclerror|all|debug|dosdebug|
  doserror|error|ikedebug|natdebug|naterror|
  packet-forwarding|pmdebug|pmerror|rulesdebug|
  ruleserror|user]
debug sole [adapters|aeroscout|algo|all|cclib|ekahau|errors|
  info|init]
```

Parameters

all	Enables debugging

cc [access-port|all|alt| ap-containment| apetect|capwap|cluster| config|dot11|eap|ids| kerberos|l3-mob|loc-ap| loc-mu|media| mobile-unit|radio|radius| self-heal|smart|snmp| system|wips|wisp|wlan] *{[debug|err|info|warn]}*	Cellcontroller (wireless) debugging message • access-port [debug|err|info|warn] – Debugs access port logs • debug – Debugs all default messages • err – Debugs error and higher severity messages • info – Debugs information and higher severity messages • warn – Debugs warning and higher severity messages • all – all modules • alt [debug|err|info|warn] – address lookup logs • ap-detect [debug|err|info|warn] – rouge AP detection logs • ap-containment [debug|err|info|warn] – rouge AP containment logs • capwap [debug|err|info|warn] – capwap logs • cluster [debug|err|info|warn] – cluster related logs • config [debug|err|info|warn] – configuration change logs • dot11 [debug|err|info|warn] – data path logs • kerberos [debug|err|info|warn] – kerberos logs • l3-mob [debug|err|info|warn] – Layer3 mobility logs • loc-ap [debug|err|info|warn] – loc-ap logs • loc-mu [debug|err|info|warn] – loc-mu logs • media [debug|err|info|warn] – encapsulation media logs • mobile-unit [debug|err|info|warn] – mobile unit logs • radio [debug|err|info|warn] – radius logs • radius [debug|err|info|warn] – radius client logs • self-heal [debug|err|info|warn] – self healing logs • smart [debug|err|info|warn] – smart-rf logs • snmp [debug|err|info|warn] – SNMP logs • system [debug|err|info|warn] – system call logs • wips [debug|err|info|warn] – WIPS sensor logs • wisp [debug|err|info|warn] – wisp logs • wlan[debug|err|info|warn] – wlan logs

ccstats <stats-module>	Cellcontroller statistics (wireless) debugging messages • stats-module [debug|error|info|warn] – Statistics Module to be debugged. • debug – Debugs all default messages • err – Debugs error and higher severity messages • info – Debugs information and higher severity messages • warn – Debugs warning and higher severity messages
certmgr [all|error|info]	Certificate manager debugging messages • all – Trace error and informational messages from Certificate Manager • error – Trace error messages from Certificate Manager • info – Trace information messages from Certificate Manager
dhcpsvr [all|error|info]	DHCP Conf Server debugging messages • all – Trace error and informational messages from DHCP Conf Server • error – Trace error messages from DHCP Conf Server • info – Trace information messages from DHCP Conf Server
imi [all|cli-client| cli-server|errors|init|ntp]	Integrated management interface debugging messages • all – All debugging • cli-client – CLI responses from Protocol modules to IMI Server • cli-server – CLI commands from IMI server to protocol module • error – errors • init – Initialization process • ntp – Net debug messages

ip [https|ssh]	Internet protocol debugging messages • https – Secure HTTP <HTTPS> Server • ssh – Secure Shell <SSH> Server
logging [all|errors|init|monitor|subagent]	Modify message logging facilities for debugging messages • all – All debugging • error – errors • init – Logging module Initialization • monitor – Logging to monitors • sub-agent – Subagent
mgmt [all|debug|err|info|sys|warning]	Management daemon debugging messages • all – All debugging • debug – Debug • info – Info • sys – System • warning –Warning • error – errors
mobility [all|cc|error|forwarding|mu|packet|peer|system]	L3 mobility debugging messages • all – All debugging <except "forwarding"> • cc – ccserver events • error – error • forwarding – Dataplane forwarding • mu –MU events and state changes • packet – Control packets • peer – Peer establishment • system – System events

mstp [all|cli|packet|protocol|timer]	*Multiple Spanning Tree Protocol* (MSTP) debugging message • all – all • cli – CLI commands • packet [rx|tx] – MSTP packets • rx – receive packet • tx – transmit packet • protocol detail – Protocol • timer detail – MSTP timers • detail – Detailed output
nsm *{[all|events|kernel|packet]}*	*Network Service Module* (NSM) debugging messages. All parameters are optional. • all – Enable all debugging • events – NSM events • kernel – NSM kernel • packet [detail|recv|send] – NSM packets • detail – Detailed information display • recv [detail] – NSM receive packets • detail – Detailed information display • send [detail] – NSM send packets • detail – Detailed information display
radius *{[all|err|info|warning]}*	RADIUS server debugging messages. All are optional parameters. • all – trace all messages from radius server • err– trace error messages from local radius server • info – trace error, warning and information messages from radius server • warn – trace error and warning messages from radius server

redundancy [all|ccmsg|config|errors| general|heartbeats|init| packets|proc|shutdown| states|subagent|timer| warnings]	Redundancy protocol debugging messages • all – Debugging all • ccmsg – Msg exchange with CC • config – Configuration processing • errors – Errors • general – General • heartbeats – Heartbeats processing • init – Redundancy initialization • packets – Packet processing • proc – Process flow • shutdown – Shutdown process • states – Redundancy states machine • subagent – Sub-agent • timer – Timer handlings • warning – Warnings

securitymgr [acldebug|aclerror|all| debug|dosdebug| doserror|error|ikedebug| natdebug|naterror| packet-forwarding| pmdebug|pmerror| rulesdebug|ruleserror| user]	Security manager debugging messages • acldebug – Trace debug messages from ACL module • aclerror – Trace error messages from ACL module • all – Trace all messages from Security Manager • debug – Trace general debug messages from Security Manager • dosdebug – Trace debug messages from DOS module • doserror – Trace error messages from DOS module • error – Trace general error messages from Security Manager • ikedebug – Trace debug messages from Ike • natdebug – Trace debug messages from NAT module • naterror – Trace error messages from NAT module • packet-forwarding <WORD> – Enable debug messages related to packet forwarding • <WORD> – Module based debug string • pmdebug – Trace debug messages from Policy Manager API calls • pmerror – Trace error messages from Policy Manager API calls • rulesdebug – Trace debug messages from rules module • ruleserror – Trace error messages from debug module • user <WORD> – Enable debug messages from Policy manager library • <WORD> – Module based debug string

sole [adapters|aeroscout|algo|all|cclib|ekahau|errors|info|init]	Location engine debugging messages • adapters – SOLE Adapter manager logs • aeroscout – Aeroscout logs • algo – Location algorithm logs • all – All module logs • cclib – cc library logs • errors – Error and higher severity logs • info – SOLE info logs • init – Initialization logs • ekahau – Ekahau logs

Example

```
RFSwitch#debug ?
  all           Enable all debugging
  cc            Cellcontroller (wireless) debugging messages
  ccstats       Cellcontroller (wireless) debugging messages
  certmgr       Certificate Manager Debugging Messages
  dhcpsvr       DHCP Conf Server Debugging Messages
  imi           Integrated Management Interface
  ip            Internet Protocol (IP)
  logging       Modify message logging facilities
  mgmt          Mgmt daemon
  mobility      L3 Mobility
  mstp          Multiple Spanning Tree Protocol (MSTP)
  nsm           Network Service Module (NSM)
  pktdrvr       Pktdrvr (kernel wireless) debugging messages
  radius        RADIUS server debugging messages
  redundancy    Redundancy Protocol debugging messages
  securitymgr   Security Manager Debugging Messages
  sole          Location engine debugging messages
RFSwitch#debug
```

4.1.11 delete

Priv Exec Command

Deletes a specified file from the system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

Parameters

/force	Forces deletion without a prompt
/recursive	Performs a recursive delete
<FILE>	Specifies the filename(s) to be deleted

Example

```
RFSwitch#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

RFSwitch#delete /force flash:/tmp.txt
RFSwitch#

RFSwitch#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
RFSwitch#
```

4.1.12 diff

Priv Exec Command

Displays the differences between 2 files

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

<FILE>	The first <FILE> is the source file for the diff. The second <FILE> is the file to compare.
<URL>	The first <URL> is the source URL for the diff. The second <URL> is the URL to compare.

Example

```
RFSwitch#diff startup-config running-config
--- startup-config
+++ running-config
@@ -89,7 +89,7 @@
  mobility peer 157.235.208.16
  wlan 1 enable
  wlan 1 ssid wlan123
- wlan 1 encryption-type wep128
+ wlan 1 encryption-type tkip
  wlan 1 authentication-type eap
  wlan 1 mobility enable
  wlan 1 radius server primary 127.0.0.1
@@ -184,10 +184,12 @@
  rad-user adam password 0 mypassword
  rad-user eve password 0 mypassword123
  rad-user sumi password 0 mypassword
+ rad-user test password 0 mypassword123
  rad-user vasavi password 0 mypassword123
  group kumar2
   rad-user sumi
-  policy wlan 2
```

```
+  policy vlan 44
+  policy wlan 10
    group kumar3
```

4.1.13 dir

Priv Exec Command

View the list of files on a filesystem

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`dir {[/all|/recursive] [<DIR>|all-filesystems]}`

Parameters

/all	Lists all files
/recursive	Lists files recursively
<DIR>	Lists files in the named file path
all-filesystems	Lists the files on all filesystems

Example

```
RFSwitch#dir
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-
config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006
cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006
cli_commands_180B.txt

RFSwitch#
```

4.1.14 disable

Priv Exec Command

Turns off the privileged mode command

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
disable
```

Parameters

None

Example

```
RFSwitch#disable
RFSwitch>
```

4.1.15 edit

Priv Exec Command

Edits a text file

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
edit <FILE>
```

Parameters

<FILE>	Name of the file to be modified

Example

```
RFSwitch#edit startup-config
GNU nano 1.2.4
startup-config

!
aaa authentication login default local none
service prompt crash-info
!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst configuration
 name My Name
!
no bridge multiple-spanning-tree enable bridge-forward
```

4.1.16 enable

Priv Exec Command

Turns on the privileged mode command

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`enable`

Parameters

None

Example

```
RFSwitch#enable
RFSwitch#
```

4.1.17 erase

Priv Exec Command

Erases a target filesystem

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
erase [nvram:|flash:|startup-config|usb1:|usb2:|cf:]
```

Parameters

nvram:	Erases everything in nvram
flash:	Erases everything in flash
startup-config	Resets the configuration to factory default
usb1:	Erases everything in usb1
usb2:	Erases everything in usb2
cf:	Erases everything in cf

Example

```
RFSwitch#erase startup-config
RFSwitch#
```

4.1.18 halt

Priv Exec Command

Stops (halts) the switch

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
halt
```

Parameters

None

Example

```
RFSwitch#halt
Wireless switch will be halted, do you want to continue?
(y/n): y
Do you want to save current configuration? (y/n/d): y
[OK]
```

4.1.19 kill

Priv Exec Command

Kills (terminates) a specified session and stops (halts) the switch

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
kill session <1-16>
```

Parameters

session	Active session (16 active sessions can be terminated)

Example

```
Telnet to switch
[xyz@xyz xyz]$ telnet

157.235.208.93
Trying 157.235.208.93...
Connected to 157.235.208.93 (157.235.208.93).
Escape character is '^]'.

RFSwitch release 3.1.0.0-XXXXXX
Login as 'cli' to access CLI.
login: root

RFSwitch#show sessions
SESSION   USER       LOCATION        IDLE
  START TIME ** 1       root   Console           00:00m

Jan  1 00:00:00 1970   2   root   157.235.208.105   00:38m
Jan  1 00:00:00 1970   3   root   157.235.208.105   00:00m
Jan  1 00:00:00 1970

RFSwitch#kill session 9
% Error: Invalid session number
RFSwitch#kill session 3
~ # Connection closed by foreign host.
[xyz@xyz xyz]$
```

4.1.20 logout

Priv Exec Command

Exits the EXEC mode and stops (halts) the switch

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
logout
```

Parameters

None

Example

```
RFSwitch#logout

RFSwitch release 3.0.0.0-200B
Login as 'cli' to access CLI.
RFSwitch login:
```

4.1.21 mkdir

Priv Exec Command

Creates a new directory in the filesystem

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mkdir <DIR>
```

Parameters

<DIR>	Directory name

Example

```
RFSwitch#mkdir TestDIR
RFSwitch#
```

4.1.22 more

Priv Exec Command

Displays the contents of a file

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
more <FILE>
```

Parameters

<FILE>	Displays the contents of the file

Example

```
RFSwitch#more flash:/log/messages.log
Sep 08 12:27:30 2006: %PM-5-PROCSTOP: Process

"radiusd" has been stopped
Sep 08 12:27:31 2006: %LICMGR-6-NEWLICENSE:

Licensed AP count changed to 48
Sep 08 12:27:31 2006: %CC-5-COUNTRYCODE:

config: setting country code to [in:
India]
Sep 08 12:27:31 2006: %DAEMON-6-INFO: radiusd

[460]: Ready to process requests.
Sep 08 12:27:35 2006: %DAEMON-6-INFO: init:

Starting pid 328, console
/dev/ttyS0
Sep 08 12:27:37 2006: %AUTH-6-INFO: login[328]:

root login  on `ttyS0' from
`Console'
Sep 08 12:27:47 2006: %IMI-5-USERAUTHSUCCESS:

User 'admin' logged in with role
```

```
of ' superuser' from auth source 'local'
Sep 08 12:28:01 2006: %NSM-6-DHCPDEFRT: Default
route with gateway
157.235.208.246 learnt via DHCP
Sep 08 12:28:01 2006: %NSM-6-DHCPIP: Interface

vlan1 acquired IP address
157.235.208.93/24 via DHCP
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11bg

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11a

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:12 2006: %MOB-6-MUADD: Station 00

-0F-3D-E9-A6-54: Added to
Mobility Database
Sep 08 12:29:12 2006: %CC-6-STATIONASSOC:
```

4.1.23 page

Priv Exec Command

Toggles switch paging. Enabling this command displays the command output page by page instead of running the entire output at once.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`page`

Parameters

None

Example

```
RFSwitch#page
RFSwitch#
```

4.1.24 ping

Priv Exec Command

Send (transmits) ICMP echo messages

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`ping {<IP>}`

Parameters

<IP>	Sets the ping destination address or hostname

Example

```
RFSwitch#ping 157.235.208.39
PING 157.235.208.39 (157.235.208.39): 100 data bytes
128 bytes from 157.235.208.39: icmp_seq=0 ttl=64 time=2.3 ms
128 bytes from 157.235.208.39: icmp_seq=1 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=2 ttl=64 time=0.3 ms
128 bytes from 157.235.208.39: icmp_seq=3 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=4 ttl=64 time=0.1 ms
--- 157.235.208.39 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.6/2.3 ms
RFSwitch#ping
Target IP address:
```

4.1.25 pwd

Priv Exec Command

View the contents of the current directory

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

pwd

Parameters

None

Example

```
RFSwitch#pwd
flash:/
RFSwitch#
```

4.1.26 quit

Priv Exec Command

Exits the current mode and moves to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
quit
```

Parameters

None

Example

```
RFSwitch#quit

RFSwitch release 4.0.0.0-XXXX
Login as 'cli' to access CLI.
RFSwitch login:
```

4.1.27 reload

Priv Exec Command

Halts the switch and performs a warm reboot

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`reload`

Parameters

None

Example

```
RFSwitch#reload
```

4.1.28 rename

Priv Exec Command

Renames a file in the existing filesystem

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rename <FILE> <FILE>
```

Parameters

<FILE>	Specifies the file to rename. The first <FILE> is the old file name. The second <FILE> is the new file name.

Example

```
RFSwitch#rename flash:/TestDIR/ NewTestDir
RFSwitch#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-
config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006
cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006
cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006
cli_commands.save
  drwx   1024      Sat Sep  2 00:31:24 2006   NewTestDir

RFSwitch#
```

4.1.29 rmdir

Priv Exec Command

Deletes an existing file from the file system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rmdir <DIR>
```

Parameters

<DIR>	Defines the name of the directory to delete

Example

```
RFSwitch#rmdir flash:/NewTestDir/
RFSwitch#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-
config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006
cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006
cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006
cli_commands.save
```

4.1.30 telnet

Priv Exec Command

Opens a telnet session

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`telnet <IP> {<port>}`

Parameters

telnet <IP> *{<port>}*	Defines the IP address or hostname of a remote system • <port> - Optional. Displays TCP Port Number

Example

```
RFSwitch#telnet 157.111.222.33

Entering character mode
Escape character is '^]'.

Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

4.1.31 terminal

Priv Exec Command

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
terminal [length <0-512>|no [length <0-512>|width]|
  width <0-512>]
```

Parameters

length <0-512>	Sets the number of lines on a screen • <0-512> – Number of lines on a screen
no [length <0-512>| width]	Negates a command or sets its defaults • length <0-512> – Unset number of lines on a screen • width – Set width of display terminal
width <0-512>	Sets the width/number of characters on a screen line • <0-512> – Number of characters on a screen

Example

```
RFSwitch>terminal length 100
RFSwitch>

RFSwitch>terminal width 200
RFSwitch>
```

4.1.32 traceroute

Priv Exec Command

Traces a route to a destination

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
traceroute [[<IP>|<hostname>]|ip [<IP>|<hostname>]]
```

Parameters

[<IP>|<hostname>]	Traces the route to a destination IP address or a hostname
ip [<IP>|<hostname>]	IP trace to a destination IP address or a hostname

Example

```
RFSwitch#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max,
38 byte packets
 1  157.235.208.39 (157.235.208.39)  0.466 ms  0.363 ms
0.226 ms
RFSwitch#
```

4.1.33 upgrade

Priv Exec Command

Upgrades the software image

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`upgrade <URL> {background}`

Parameters

<URL>	Location of the target firmware image used in upgrade
background	Optional. Specifies that the upgrade should occur in the background.

Example

```
RFSwitch#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

update is /dev/hda6
Reading image file header
Removing other partition
Sep 08 15:57:18 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Making file system
Extracting files (this can take some time).Sep
.........................
Jan 08 15:58:17 2009: %DIAG-4-CPULOAD: One
minute average load limit exceeded,
value is 100.00% limit is 99.90% (top process
kernel/ISR 100.00%)
Sep 08 15:58:44 2009: %PM-4-PROCNORESP: Process
```

```
"logd" is not responding
Jan 08 15:58:44 2009: %PM-4-PROCNORESP: Process

"logd" is not responding
Jan08 15:58:44 2009: %PM-4-PROCNORESP: Process
"logd" is not responding
Jan 08 15:58:44 2009: %PM-4-PROCNORESP: Process

"logd" is not responding
Version of firmware update file is 4.0.0.0-03D
19193X
Jan08 15:58:44 2009: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Creating LILO files
Running LILO
Successful
Jan 08 15:58:46 2009: %FWU-6-FWUDONE: Firmware

update successful, new version is 4.0.0.0-038D
RFSwitch#
```

4.1.34 upgrade - abort

Priv Exec Command

Aborts an ongoing upgrade process

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`upgrade-abort`

Parameters

None

Example

```
RFSwitch#upgrade-abort
```

4.1.35 write

Priv Exec Command

Writes the running configuration to memory or a terminal

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
write [memory|terminal]
```

Parameters

memory	Writes to NV memory
terminal	Writes to terminal

Example

```
RFSwitch#write terminal
!
! configuration of RFSwitch version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1
45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
```

```
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
!.....................................
```

4.1.36 format

Priv Exec Command

Formats file system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
format cf:
```

Parameters

cf:	Formats compact flash

Example

```
RFSwitch#format cf:
```

5

Global Configuration Commands

The term global is used to indicate characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The example below describes the process of entering the global configuration mode from privileged EXEC mode:

```
RFSwitch# configure terminal
RFSwitch(config)#
```



NOTE: The system prompt changes to indicate you are now in global configuration mode. The prompt for global configuration mode consists of the device host name followed by (config) and the pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC command is issued.

5.1 Global Configuration Commands

Table 5.1 summarizes the Global Config commands

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
aaa	Configures the current authentication, authorization and accounting (aaa) login settings	*page 5-5*
access-list	Adds an access list entry	*page 5-7*
autoinstall	Autoinstalls a configuration command	*page 5-14*
banner	Defines a login banner	*page 5-16*
boot	Reboots the switch	*page 5-17*
bridge	Displays bridge group commands	*page 5-18*
clrscr	Clears the display screen	*page 2-2*
country-code	Configures the country of operation. All existing radio configuration will be erased	*page 5-21*
crypto	Defines encryption parameters	*page 5-22*
do	Runs commands from the EXEC mode	*page 5-39*
end	Ends the current mode and moves to the EXEC mode	*page 5-40*
errdisable	Recovers from errors	*page 5-41*
exit	Ends the current mode and moves to the previous mode	*page 2-3*
ftp	Configures FTP server parameters	*page 5-42*
help	Describes the interactive help system	*page 2-4*
hostname	Sets the system's network name	*page 5-43*
interface	Defines an interface to configure	*page 5-44*
ip	Internet Protocol (IP)	*page 5-46*

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
license	Sets license management commands	*page 5-58*
line	Configures a terminal line	*page 5-59*
local	Sets the username and password for local user authentication	*page 5-60*
logging	Modifies message logging facilities	*page 5-61*
mac	Configures MAC access-lists	*page 5-64*
mac-address-table	Configures MAC address table	*page 5-65*
mac-name	Sets a name to the MAC address of a MU	*page 5-66*
management	Sets properties of the management interface	*page 5-67*
no	Negates a command or set its defaults	*page 2-5*
ntp	Configures *Network Time Protocol* (NTP) parameters	*page 5-68*
prompt	Sets the system prompt	*page 5-73*
radius-server	Enters the RADIUS server mode	*page 5-74*
ratelimit	Sets the rate limit feature parameters	*page 5-76*
redundancy	Configures redundancy group parameters	*page 5-77*
role	Sets the Role Based Firewall parameters	*page 5-80*
rtls	Configures Real Time Location System parameters	*page 5-82*
show	Displays the running system information	*page 2-37*
service	Service commands	*page 5-83*
smtp-notification	Modifies SMTP notification parameters	*page 5-86*
snmp-server	Modifies SNMP engine parameters	*page 5-94*

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
spanning-tree	Configures spanning tree commands	*page 5-107*
timezone	Configures the timezone	*page 5-111*
traffic-shape	Configures traffic shaping	*page 5-112*
username	Establishes user name authentication	*page 5-115*
vpn	Defines the VPN configuration	*page 5-118*
wireless	Configures wireless parameters	*page 5-119*
wlan-acl	Applies an ACL on WLAN	*page 5-120*
network-element-id	Sets system's network element ID	*page 5-123*
firewall	Configures Wireless firewall	*page 5-124*

5.1.1 aaa

Global Configuration Commands

Configures the current *Authentication, Authorization and Accounting* (AAA) login settings

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
aaa [authentication|nas|vpn-authentication]

aaa authentication login default [local|none|radius]
aaa nas <name>
aaa vpn-authentication [primary|secondary] <IP> key [0
<secret>|2 <secret>|<secret>] {authport <1024-65535>}
```

Parameters

authentication login default [local|none|radius]	Sets the authentication configuration parameters. • login – Sets the authentication lists for login • default – Defines the default authentication list • local – Sets the local user database • none – No authentication • radius – Defines an external RADIUS server
nas <name>	Sets the NAS identifier. The <name> parameter accepts a string of 64 characters.

vpn-authentication [primary|secondary] [<IP> key [0 <secret>| 2 <secret>|<secret>] *{authport <1024-65535>}*	Sets the configuration for VPN authentication using RADIUS. • primary – Sets the configuration for the primary server. • secondary – Sets the configuration for the secondary server. • key [0 <secret>|2 <secret>|<secret>] – Sets the secret key settings. • 0 <secret> – Indicates that the password is specified unencrypted. • 2 <secret> – Indicates that the password is encrypted with password-encryption secret. • <secret> – A shared secret up to 32 characters. • authport <1024-65535> – Sets an optional RADIUS Server authentication port

Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server

5.1.2 access-list

Global Configuration Commands

Adds an *Access List* (ACL) entry. Use the `access-list` command (under Global Configuration) to configure the access list mechanism for filtering frames by protocol type or vendor code.

ACLs control access to the network through a set of rules. Each rule specifies an action which is taken when a packet matches it within the given set of rules. If the action is *deny*, the packet is dropped and if the action is *permit*, the packet is allowed. The switch supports the following ACLs:

- IP Standard ACLs
- IP Extended ACLs
- MAC Extended ACLs

ACLs are identified by either a number or a name. Numbers are predefined for IP Standard and Extended ACLs, and the name can be any valid alphanumeric string (not exceeding 64 characters). With numbered ACLs, the rule parameters have to be specified on the same command line along with the ACL identifier.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>]
```

For Standard IP ACLs:

```
access-list [<1-99>|<1300-1999>] [deny|permit|mark]
access-list [<1-99>|<1300-1999>] deny [<IP/MASK>|any|
  host <IP>] {[rule-precedence <1-5000>|
  log {rule-precedence <1-5000>}]}
access-list [<1-99>|<1300-1999>] permit [<IP/MASK>|any|
  host <IP>] {[rule-precedence <1-5000>|
  log {rule-precedence <1-5000>}]}
access-list [<1-99>|<1300-1999>] mark [8021p <0-7>|
dscp <0-63>|tos <0-255>] [<IP/MASK>|any|host <IP>]
{[rule-precedence <1-5000>|log {rule-precedence <1-5000>}]}
```

For Extended IP ACLs:

`access-list [<100-199>|<2000-2699>] [deny|permit|mark]` `[icmp|ip|tcp|upd]`

`access-list [<100-199>|<2000-2699>] [deny|permit|mark] icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}`

`access-list [<100-199>|<2000-2699>] [deny|permit|mark]ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {log} {rule-precedence <1-5000>}`

`access-list [<100-199>|<2000-2699>] [deny|permit|mark] [tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq <source-port>|range <starting-source-port> <ending-source-port>} [<dest-IP/Mask|any|host <IP>] {eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}`



NOTE Using `access-list [<100-199>|<2000-2699>]` moves you to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Instance on page 14-1*.

Using `access-list [<1-99>|<1300-1999>]` moves you to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Instance on page 15-1*.

To create a named ACL, use `ip access-list` (Standard/Extended). For more information, see *ip on page 5-46*.

Parameters

access-list [<1-99>|<1300-1999>] [permit|deny] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds a standard access list entry. • [<1-99>|<1300-1999>] – Defines access list number from 1-99 or 1300-1999. • [deny|permit] – Defines action types on an ACL. • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter.

access-list [<1-99>|<1300-1999>] mark [8021p <0-7>|dscp <0-63>|tos <0-255>] [<IP/MASK>|any|host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds a standard access list entry. • [<1-99>|<1300-1999>] – Defines access list number from 1-99 or 1300-1999. • mark – Marks a packet. The action type **`mark`** is functional only over a Port ACL. • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values. • dscp <0-63> – Used only with the action type `mark` to specify DSCP values. • tos <0-255> – Used only with the action type `mark` to specify *type of service* (tos) values. • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter.

access-list [<100-199>|<2000-2699>] [permit|deny] [icmp|ip|tcp|udp] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds an Extended IP access list entry. • (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL must be between 2000-2699 • [deny|permit] – Defines action types on an ACL. • [icmp|ip|tcp|udp] – The protocol type for the extended ACL entry. • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter.

access-list [<100-199>|<2000-2699>] mask [8021p <0-7>|dscp <0-63>|tos <0-255>] [icmp|ip|tcp|udp] [<IP/MASK>|any| host <IP>] *{[rule-precedence <1-5000> {log}|log]}*	Adds an Extended IP access list entry. • (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL must be between 2000-2699 • mark – Marks a packet. The action type `mark` is functional only over a Port ACL. • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values. • dscp <0-63> – Used only with the action type `mark` to specify DSCP values. • tos <0-255> – Used only with the action type `mark` to specify *type of service* (tos) values. • [icmp|ip|tcp|udp] – The protocol type for the extended ACL entry. • [<IP/MASK>| host <IP>| any] – <IP/MASK> is the source address of the network or host in dotted decimal format. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. This is an optional parameter • rule-precedence <1-5000> – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL. This is an optional parameter.

Use an access list command under the global configuration to create an access list. The switch supports port, router and WLAN ACLs

- When the access list is applied on an Ethernet port, it becomes a port ACL
- When the access list is applied on a VLAN interface, it becomes a router ACL
- When the access list is applied on a WLAN index, it becomes a WLAN ACL

A MAC access list (to allow arp), is mandatory for both port and WLAN ACL's. For more information on how to configure a MAC access list, see *permit on page 16-15*.

Example

The example below creates a standard access list (ACL) to permit any traffic coming to the interface:

```
RFSwitch(config)#access-list 1 permit any
RFSwitch(config)#
```

The example below creates a extended IP access list to permit IP traffic between two networks:

```
RFSwitch(config)#access-list 101 permit ip 192.168.1.0/24
192.168.2.0/24

RFSwitch(config)#
```

The example below creates a extended access list to permit tcp traffic, between two networks, with destination port range between 20 and 23:

```
RFSwitch(config)#access-list 101 permit tcp 192.168.1.0/24
192.168.2.0/24 range 20 23
RFSwitch(config)#
```

The example below denies icmp traffic from any source to any destination:

```
RFSwitch(config)#access-list 115 deny icmp any any
RFSwitch(config)#access-list 115 permit ip any any
RFSwitch(config)#
```

5.1.3 autoinstall

Global Configuration Commands

Autoinstalls the switch image

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
autoinstall [clear-config-history|cluster-config|config|
  image|reset-config|start]
autoinstall [clear-config-history|reset-config|start]
autoinstall [cluster-config|config] {url <URL>}
autoinstall image {[url <URL>|version <version>]}
```

Parameters

clear-config-history	Autoinstalls a clear configuration history, resulting in a reversion.
cluster-config *{url <URL>}*	Autoinstalls a cluster-config setup. • url – Optional. Sets the URL of the item. • <URL> – Remote/external location of the file URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file

config *{url <URL>}*	Autoinstalls a config setup. • url – Optional. Sets the URL of the item. • URL – Remote/external location of the file. URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file
image *{[url <URL>| version <version>]}*	Autoinstalls the image setup. • url – Optional. Sets the URL of the item. • <URL> – Remote/external location of the file. URLS: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • version <version> – The version number <version> cannot be the same as the currently installed version number. Attempting to install the same version results in an unsuccessful download
reset-config	Resets all autoinstall features to factory defaults
start	Starts the autoinstall sequence

Example

```
RFSwitch(config)#autoinstall clear-config-history
RFSwitch(config)#
```

5.1.4 banner

Global Configuration Commands

Defines a login banner for the switch. Use `{no} banner` to delete a previously configured banner.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
{no} banner motd [<message>|default]
```

Parameters

motd [<message>| default]	Sets the *message of the day* (MOTD) banner. <message> is the custom message to be displayed.Use default to set the MOTD string to the default message for the switch.

Usage Guidelines

Use **`no banner motd`** to delete the previously configured banner.

Example

```
RFSwitch(config)#banner motd Welcome to my RFSwitch CLI
RFSwitch(config)

RFSwitch release 3.1.0.0-XXXX
Login as 'cli' to access CLI.
RFSwitch login: cli
Welcome to my RFSwitch CLI
Welcome to my RFSwitch CLI
RFSwitch>

RFSwitch release 3.0.2.0-003B
Login as 'cli' to access CLI.
RFSwitch login: cli
Welcome to CLI
Welcome to CLI

RFSwitch>
```

5.1.5 boot

Global Configuration Commands

Reboots the switch with an image in the mentioned partition (either the primary or secondary partition)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
boot system [primary|secondary]
```

Parameters

system [primary|secondary]	Specifies the boot image used after reboot • primary – Specifies the primary image • secondary – Specifies the secondary image

Example

```
RFSwitch(config)#boot system primary
Wireless switch will be rebooted, do you want to continue?
(y/n):y
Do you want to save the configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

5.1.6 bridge

Global Configuration Commands

Configures bridge specific commands

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The interfaces mentioned below are supported in the following platforms:

- ge <index> – RFS7000 supports 4 GEs and RFS6000 supports 8 GEs
- sa <1-4> – Only supported on RFS7000
- me1 – Only supported on RFS7000 and RFS6000
- up1 – Only supported on RFS6000

Syntax

```
{no} bridge [<bridgegroup>|multiple-spanning-tree]

bridge <bridegegroup> [address|ageing-time]
bridge  <bridegegroup> address <MAC> [discard|forward]
[<interface>|ge <1-8>|me1|sa <1-4>|up1|vlan <1-4094>]
bridge <bridegegroup> ageing-time [0|<10-1000000>]

bridge multiple-spanning-tree enable
```

Parameters

bridge <bridge-group> address <MAC> [discard|forward] [<interface>|ge <1-8>| me1|sa <1-4>|up1| vlan <1-4094>] bridge <bridge-group> ageing-time [0|<10-1000000>]	Bridge groups available for bridging. • <bridgegroup> – Bridge group value between 1 and 32. • address <MAC> – Unique hardware address in the HHHH.HHHH.HHHH format. • [discard|forward] – Either discard or forward the interface on which the configured rule is applied. This filter frames on a specific interface that contain the specified hardware address in either the source or destination field. • <interface> – The name of the interface • vlan <2-4094> – VLAN interface • ge <index> – Gigabit Ethernet interface. RFS7000 supports 4 GE's and RFS6000 supports 8 GEs • sa <1-4> – Static Aggregate interface index. Only supported on RFS7000 • me1 – Fast Ethernet interface. • up1 – WAN interface. Only available on RFS6000 • ageing-time [0|<10-1000000>] – The time duration a learned MAC address persists after the last update • 0 – Disables aging • <10-1000000> – Sets aging time in seconds
multiple-spanning-tree enable	Enables *Multiple Spanning Tree Protocol* (MSTP) commands

Usage Guidelines

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment. Use multiple bridge address discard/forward commands to develop the filter scheme.

Use the `(no)bridge [<1-32>|multiple-spanning-tree]`command to delete the configured discard or forward filters.

Example

```
RFSwitch(config)#bridge multiple-spanning-tree enable
RFSwitch(config)#
```

```
RFSwitch(config)#bridge 2 address 1a2b:3c4d:5e6f forward eth
1 vlan 2
RFSwitch(config)#
```

5.1.7 country-code

Global Configuration Commands

Sets the country of operation

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
{no} country-code <code>
```

Parameters

<code>	A two (2) letter ISO-3166 country code. To view country codes, use the `show wireless country-code-list` command.

Usage Guidelines

`{no} country-code` erases all existing radio configuration.

Example

```
RFSwitch(config)#country-code ?
  WORD  the 2 letter ISO-3166 country code ("show wireless
country-code-list" to see list of supported countries)

RFSwitch(config)#no country-code US
RFSwitch(config)#
```

5.1.8 crypto

Global Configuration Commands

Use crypto to define system level local ID for ISAKMP negotiation and to enter the ISAKMP Policy, ISAKMP Client or ISAKMP Peer command set.



NOTE: `crypto isakmp(policy)Priority` moves to the `config-crypto-isakmp` instance. For more information, see *Crypto-isakmp Instance on page 6-1*.

`crypto isakmp client configuration group default` moves you to the `config-crypto-group` instance. For more details, see *Crypto-group Instance on page 7-1*.

`crypto isakmp peer IP Address` moves to the `config-crypto-peer` instance. For more details, see *Crypto-peer Instance on page 8-1*.

`crypto ipsec transformset <tag> <value>` leads you to `crypto-ipsec.` Use the crypto ipsec transform-set command to define the transform configuration for securing data (for example, esp-3des, esp-sha-hmac, etc.). The transform-set is assigned to a crypto map using the map's set transform-set command. For more details, see *Crypto-ipsec Instance on page 9-1*.

`crypto pki trustpoint` mode leads to the `config-trustpoint` instance. For more details, see *Crypto-trustpoint Instance on page 11-1*.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
crypto [ipsec|isakmp|key|map|pki]

crypto ipsec [security-association|transform-set]
crypto ipsec security-association lifetime
  [kilobyte|seconds] <lifetime>
crypto ipsec transform-set <transform-set-tag>
  [ah-md5-hmac|ah-sha-hmac|esp-3des|esp-aes|esp-aes-192|
  esp-aes-256|esp-des|esp-md5-hmac|esp-sha-hmac]
```

```
crypto isakmp [client|keepalive|key|peer|policy]
crypto isakmp client configuration group default
crypto isakmp keepalive <10-3600>
crypto isakmp key [0 <secret>|2 <secret>|<secret>]
  [address <IP>|hostname <HOST>]
crypto isakmp peer [address <IP>|dn <distinguished-name>|
  hostname <HOST>]
crypto isakmp policy <1-10000>

crypto key [export|generate|import|zeroize]
crypto key export rsa <rsa-keypair> <URL> {<pass-phrase>}
crypto key generate rsa <rsa-keypair-name> <1024-2048>
crypto key import rsa <rsa-keypair-name> <URL>
  {<pass-phrase>}
crypto key zeroize rsa <rsa-keypair-name>

crypto map <crypto-map-tag> <1-1000> [ipsec-isakmp|ipsec-
manual] {dynamic}

crypt pki [authenticate|enroll|export|import|trustpoint]
crypto pki authenticate <trust-point-name> [terminal|<URL>]
crypto pki enroll <trust-point-name> [request|self-signed]
crypto pki export <trust-point-name> [request|trustpoint]
  <URL>
crypto pki import <trust-point-name> [certificate|crl|
trustpoint]
crypto pki import <trust-point-name> certificate
  [<URL>|terminal]
crypto pki import <trust-point-name> crl <URL> <

crypto pki(authenticate|enroll|export|import|trustpoint)
crypto pki authenticate <name> (terminal|URL)
crypto pki enroll<name> (request|self-signed)
crypto pki [import|export] <name> (request|trustpoint)(URL)
crypto pki import ads [certificate|crl|trustpoint]
(URL)(terminal)
```

Parameters

ipsec (security-association| transform-set)	Configures IPSEC policies. • security-association – Defines the security association parameter used to define its lifetime. • lifetime (kilobyte | seconds) – The lifetime of IPSEC security association. It can be defined in either: *kilobytes* – Volume-based key duration, the minimum is 500 KB and maximum is 2147483646 KB . *seconds* – Time-based key duration, the minimum is 90 seconds and maximum is 2147483646 seconds. • transform-set [set name] – Uses the crypto ipsec transform-set command to define the transform configuration (authentication and encryption) for securing data. • ah-md5-hmac • ah-sha-hmac • esp-3des • esp-aes • esp-aes-192 • esp-aes-256 • esp-des • esp-md5-hmac • esp-sha-hmac The transform-set is then assigned to a crypto map using the map's set transform-set command. For more information, see *Crypto-map Instance on page 10-1*.

isakmp [client|keepalive|key| peer|policy]	Configures the *Internet Security Association and Key Management Protocol* (ISAKMP) policy. • client configuration (group) (default) – Leads to the config-cryptogroup instance. For more details see *Crypto-group Instance on page 7-1*. • keepalive <10-3600> – Sets a keepalive interval for use with remote peers. It defines the number of seconds between DPD messages. • key [0 <key>|2 <key>|<key>] [address|hostname] – Sets a pre-shared key for remote peer. • 0 <key> – Password is specified unencrypted. • 2 <key> – Password is encrypted with password-encryption secret • <key> – User provided password. • address – Defines a shared key with an IP address. • hostname – Defines the shared key with a hostname. • peer [address|dn|hostname] – Sets the remote peer. • address – The IP address is the identity of the remote peer. • dn – The identity of the remote peer is the distinguished name. • hostname –The hostname is the identity of the remote peer. • policy <1-10000> – Sets a policy for a ISAKMP protection suite.

key [export|generate|import| zeroize]	Authentication key management functions. • export rsa <name> URL [tftp|ftp] – Exports a keypair related configuration. • generate rsa <name> <1024-2048> – Generates a keypair. • <1024-2048> – Size of keypair in bits. • import rsa <name> URL [tftp|ftp] – Imports keypair related configuration • zeroize rsa <name> – Deletes a keypair. • rsa <identifier> – RSA keypair identifier associated with keypair. • URL for sending the key, it can be one of the following: • tftp://<IP>/path/file (or) • ftp://<user>:<passwd>@<IP>/path/file
map <name> <sequence> [ipsec-isakmp| ipsec-manual] dynamic	Enter a crypto map. For more information, see *Crypto-map Instance on page 10-1*. • name <name> – Names the crypto map entry (not to exceed 32 characters) . • <1-1000> – Sequence to insert into crypto map entry. • ipsec-isakmp – IPSEC w/ISAKMP. • ipsec-manual – IPSEC w/manual keying. • dynamic – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration.

pki [authenticate|enroll| export|import|trustpoint]	Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities. The PKI ensures each online party is who they claim to be. • authenticate <name> (terminal|tftp|ftp) – Defines the authenticate and import CA certificate. • enroll <name> (request|self-signed) – Generates a certificate request or selfsigned certificate for the trustpoint. • export <name> (request|trustpoint) (tftp|ftp) – Exports the trustpoint related configuration. • import – Imports a trustpoint related configuration. • certificate – Imports server certificate for the trust point. • crl – certificate Revocation list. • URL – URL to get certificate from URLS: tftp://<IP>/path/file ftp://<user>:<passwd>@<IP>/path/file • terminal – Copy and paste mode of enrollment. • trustpoint – Import trust point including either private key and server certificate or ca certificate or both. • trustpoint – Creates and configures a trustpoint.

Usage Guidelines

Follow the table to calculate how many character are required to add the key size for authentication and encryption. This is used while configuring Manual IPSEC only.

		AH-MD5	AH-SHA							
AH		32	40							
		ESP-MD5			ESP-SHA					
ESP-AUTH		Cipher	Auth		Cipher	Auth				
		16	16		20	20				
	DES		3DES		AES		AES-192		AES-256	
ESP-ENCR	Cipher	Auth	Cipher	Auth	Cipher	Auth	Cipher	Auth	Cipher	auth
	8	8	24	24	16	16	16	16	16	16

For example, To create a key with authentication type as ESP-SHA and encryption type as AES-192, enter 20+16=36 characters.

The key size for all the 3 different AES combinations is 128 bits or 16 bytes.

Follow the example below to see how the Auth and Encryption key is created in `(config)# crypto-ipsec` instance and used in `(config)# crypt-map` instance.

```
RFSwitch(config)#crypto ipsec transform-set Test1 ?
  ah-md5-hmac    AH-HMAC-MD5 transform
  ah-sha-hmac    AH-HMAC-SHA transform
  esp-3des       ESP transform using 3DES cipher (168 bits)
  esp-aes        ESP transform using AES cipher
  esp-aes-192    ESP transform using AES cipher (192 bits)
  esp-aes-256    ESP transform using AES cipher (256 bits)
  esp-des        ESP transform using DES cipher (56 bits)
  esp-md5-hmac   ESP transform using HMAC-MD5 auth
  esp-sha-hmac   ESP transform using HMAC-SHA auth

RFSwitch(config)#crypto ipsec transform-set Test1 esp-aes-
192 esp-sha-hmac

RFSwitch(config-crypto-ipsec)#exit

RFSwitch(config)#crypto map TestMap-TechPub 10 ipsec-manual
RFSwitch(config-crypto-map)#set peer 1.1.1.1
RFSwitch(config-crypto-map)#match  address 101

RFSwitch(config-crypto-map)#set transform-set tfset-manual
```

```
RFSwitch(config-crypto-map)#set session-key inbound esp 257
cipher 1234567890123456789012345678901234567890123456
authenticator 1234567890123456789012345678901234567890123456


RFSwitch(config-crypto-map)#set session-key outbound esp 258
cipher 1234567890123456789012345678901234567890123456
authenticator 1234567890123456789012345678901234567890123456

RFSwitch(config-crypto-map)#exit

RFSwitch(config)#interface vlan11

RFSwitch(config-if)#crypto map manual


RFSwitch(config-if)#show running-config
!
! configuration of RFS7000 version 1.2.0.0-024D  version 1.1
!
!
aaa authentication login default none
service prompt crash-info
!
username "admin" password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d

username "admin" privilege  superuser
username "operator" password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 30 deny 11.1.1.0/24 log rule-precedence 10
access-list 101 permit ip 12.1.1.0/24 10.1.1.0/24 rule-
precedence 10
access-list 102 permit ip 22.1.1.0/24 20.1.1.0/24 rule-
precedence 10
mac access-list extended 200
permit any any type arp rule-precedence 10
!
.....................................................
.....................................................
.....................................................
.............
crypto isakmp key 0 12345678 address 11.1.1.1
```

```
crypto isakmp key 0 12345678 address 21.1.1.1
.....................................................
.
.....................................................
.
crypto ipsec transform-set tfset1 esp-3des esp-sha-hmac
mode tunnel
crypto ipsec transform-set tfset-manual esp-3des esp-sha-
hmac
mode tunnel
!
crypto map MAP1 10 ipsec-isakmp
set peer 11.1.1.1
match address 101

set transform-set tfset1
set security-association level perhost
set security-association lifetime seconds 120
set security-association lifetime kilobytes 4608000
crypto map MAP2 10 ipsec-isakmp

set peer 21.1.1.1
match address 102


set transform-set tfset1
set security-association level perhost
set security-association lifetime seconds 120
set security-association lifetime kilobytes 4608000
crypto map remote 10 ipsec-isakmp dynamic

set peer 0.0.0.0
set remote-type xauth
crypto map manual 10 ipsec-manual
set peer 1.1.1.1
set session-key in esp 257 cipher
12345678901234567890123456789012345678901234 authenticator
12345678901234567890123456789012345678901234

set session-key out esp 258 cipher
12345678901234567890123456789012345678901234 authenticator
12345678901234567890123456789012345678901234

match address 101
```

```
set transform-set tfset-manual
!
.....................................................
.
.....................................................
.
interface vlan11
ip address 11.1.1.2/24
crypto map manual
!
.....................................................
.
.....................................................
.
RFSwitch(config-if)#
```

Usage Guidelines

A peer address can be deleted with a wrong isakmp value. Crypto currently matches only the IP address when a **no** command is issued

```
RFSwitch(config)#crypto isakmp key 12345678 address 4.4.4.4

RFSwitch(config)#show running-config
configuration of RFSwitch version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1
45b27d6483fc630981ad5096ff26a7956ce0c038
.......................................
.............................
crypto isakmp key 12345678 address 4.4.4.4
crypto ipsec security-association lifetime kilobytes 4608000
RFSwitch(config)#

RFSwitch(config)#no crypto isakmp key 12348 address 4.4.4.4
RFSwitch(config)#
```

In the example above, **key 12345678** is associated with IP **address 4.4.4.4**. You can delete this key by using the no command and a wrong key number

Example

```
RFSwitch(config)#crypto pki ?
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

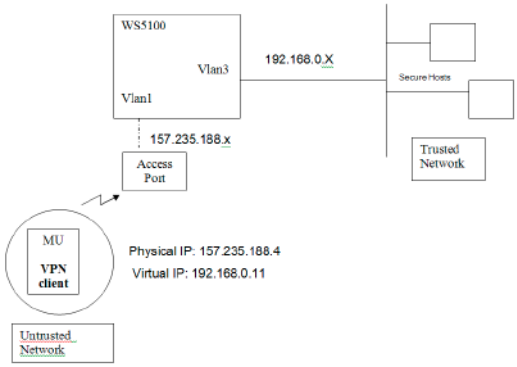
RFSwitch(config)#crypto pki trustpoint ?
  WORD  Trustpoint Name

RFSwitch(config)#crypto pki trustpoint Test
RFSwitch(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for
request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required
parameters                to configure a trustpoint.

RFSwitch(config-trustpoint)#
```

5.1.8.1 Use Case 1: Configuring Remote VPN

Let us review an example of a mobile unit connected to the switch. Assume it wants access to the corporate (trusted network) using IPSec VPN functionality.



In the figure above, a Motorola client is associated to a WLAN (say wlan1) attached to vlan2 on the switch. vlan2 is on subnet 10.1.1.x and is running a DHCP server that assigns IP addresses for this subnet. The corporate is on vlan3 of the switch, which has 192.168.0.x subnet.

The client being associated to wlan1 has an IP address of 10.1.1101x and wants to access the 192.168.0.x network securely.

In case the client is VPN enabled, it initiates a connection with the VPN server on our switch, the “conversation” that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE *Extended Authentication* (Xauth), push client relate configuration (using Mode Configuration), and IPsec security association (SA) creation.

Depending on the switch IPSec configuration (as discussed in the previous sections), the client establishes an IKE SA, and if the switch is configured for Xauth, the client waits for a "username/password" challenge and then responds to the challenge of the switch.

If the switch indicates that authentication is successful, the client requests further configuration parameters from the switch. At this stage, the private IP address (mode-config) is pushed to the client from a private address pool, configured for remote VPN clients. IPsec SA’s are created and the connection is complete.

Once the client has got a virtual IP, further packets from the client within the IPSec tunnel are routed to the corresponding VLAN interface (in our case vlan3), and the client gets

access to the network. The IPSec tunnel is only between the client and the switch. After that the packets on the trusted side are sent without encryption.



NOTE: The example below is for a IPSec-L2TP connection over a mobile unit. Use a windows default client for this configuration.

1. Create and configure a WLAN.

```
RFSwitch(config)#
RFSwitch(config)#wireless
RFSwitch(config-wireless)#wlan 2 enable
RFSwitch(config-wireless)#wlan 2 ssid MONARCH2
RFSwitch(config-wireless)#wlan 2 vlan 2
```

2. Create and configure DHCP.

```
RFSwitch(config)#ip dhcp pool vlan2
RFSwitch(config-dhcp)#address range 10.1.1.2 10.1.1.254
RFSwitch(config-dhcp)#default-router 10.1.1.1
RFSwitch(config-dhcp)#network 10.1.1.0/24
```

3. Create and configure a VLAN interface named vlan2.

```
RFSwitch(config)#interface vlan2
RFSwitch(config-if)#ip address 10.1.1.1/24
```

4. Create and configure another VLAN interface named vlan3.

```
RFSwitch(config)#interface vlan 3
RFSwitch(config-if)#ip address dhcp
```

Use the commands below to configure IPSec VPN on the switch:

1. Create an Extended ACL.

```
RFSwitch(config-ext-nacl)#ip access-list extended 101
```

2. Configure the local subnet and remote subnet as interesting traffic.

```
RFSwitch(config-ext-nacl)# permit ip 10.1.1.0/24 any
RFSwitch(config-ext-nacl)# permit ip 192.168.0.0/24 any
```

3. Configure a private pool address.

```
RFSwitch(config)# ip local pool lo 192.168.0.2 hi 192.168.0.10
```

4. Specify DNS/WINS for the remote client.

```
RFSwitch(config)#crypto isakmp client configuration group
default
```

```
RFSwitch(config-crypto-group)#dns 10.1.1.1
RFSwitch(config-crypto-group)#wins 10.1.1.1
```

5. Specify the authentication type.

```
RFSwitch(config)# aaa vpn-authentication local
RFSwitch(config)# local username harry password symbol123
```

6. Create a transform set.

```
RFSwitch(config)#crypto ipsec transform-set windows esp-3des
esp-sha-hmac
RFSwitch(config-crypto-ipsec)#mode transport
```

7. Specify a dynamic crypto map.

```
RFSwitch(config)#crypto map TestMap 30 ipsec-isakmp dynamic
RFSwitch(config-crypto-map)#set peer 0.0.0.0
RFSwitch(config-crypto-map)#match address 101
RFSwitch(config-crypto-map)#set transformset windows
RFSwitch(config-crypto-map)#set remote-type ipsec-l2tp
```

8. Apply the crypto map to interface vlan2.

```
RFSwitch(config)#interface vlan2
RFSwitch(config-if)cryto map TestMap
```

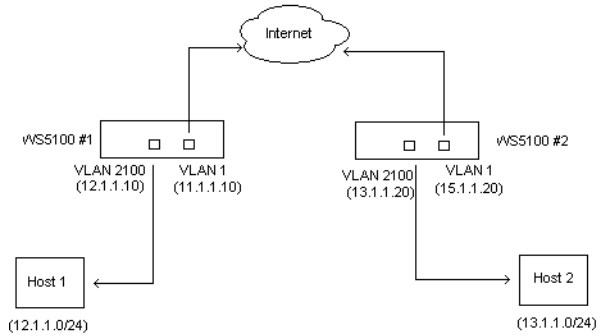
9. Upon a successful connection, the XP client will obtain a virtual IP address.

5.1.8.2 Use Case 2: Configuring Site-to-Site VPN

Intranets use unregistered addresses connected over the public internet by site-to-site VPN. In this scenario, NAT is required for the connections to the public internet. However NAT is not required for traffic between the two intranets, which can be transmitted using a VPN tunnel over the public Internet.

The site-to-site VPN allows branch office mobility controllers to connect back to the central office using a secure, encrypted tunnel, for all site-to-site traffic. This allows a

wired LAN in the branch office to bridge directly to the central site while maintaining full security.



This example requires two switches. It can be configured with the following commands:

1. Configuration required on switch 1:

   a.Create an extended ACL. This is used to define the tunnel used by the traffic.

   ```
   RFSwitch(config)#access-list 150 permit ip 12.1.1.0/24
   13.1.1.0/24 rule-precedence
   ```

   b.Create and configure ISAKMP parameters.

   ```
   RFSwitch(config)#crypto isakmp keepalive 10
   RFSwitch(config)#crypto isakmp key SYMBOLAD address
   15.1.1.20
   RFSwitch(config)#crypto ipsec security-association lifetime
   kilobytes 4608000
   ```

   c.Create and configure ISAKMP policy.

   ```
   RFSwitch(config)#crypto isakmp policy 199
   RFSwitch(config-crypto-isakmp)#encryption aes
   RFSwitch(config-crypto-isakmp)#hash sha
   RFSwitch(config-crypto-isakmp)#authentication pre-share
   RFSwitch(config-crypto-isakmp)#group 5
   RFSwitch(config-crypto-isakmp)#lifetime 9496
   ```

   d.Create and configure an IPSec transform set.

   ```
   RFSwitch(config)#crypto ipsec transform-set TFSET ah-sha-
   hmac esp-aes
   ```

```
RFSwitch(config-crypto-ipsec)#mode tunnel
```

e.Create and configure a crypto map.

```
RFSwitch(config)#crypto map THIRDMAP 435 isakmp
RFSwitch(config-crypto-map)#set peer 15.1.1.20
RFSwitch(config-crypto-map)#match address 150
RFSwitch(config-crypto-map)#set transformset TFSET
RFSwitch(config-crypto-map)#set security-association
lifetime seconds 3600
```

f.Associate the crypto map with a VLAN interface.

```
RFSwitch(config)#interface vlan1
RFSwitch(config-if)#ip address 11.1.1.10/24
RFSwitch(config-if)#crypto map THIRDMAP
RFSwitch(config-if)#interface vlan2100
RFSwitch(config-if)#ip address 12.1.1.10/24
RFSwitch(config-if)#ip route 0.0.0.0/0 11.1.1.2
```

2. Configuration required on switch 2:

a.Create an extended ACL. This is defines the tunnel used by the traffic.

```
RFSwitch(config)#access-list 155permit ip 13.1.1.0/24
12.1.1.0/24 rule-precedence 1
```

b.Create and configure the ISAKMP parameters.

```
RFSwitch(config)#crypto isakmp keepalive 10
RFSwitch(config)#crypto isakmp key SYMBOLAD address
11.1.1.10
RFSwitch(config)#crypto ipsec security-association lifetime
kilobytes 4608000
```

c.Create and configure ISAKMP policy.

```
RFSwitch(config)#crypto isakmp policy 100
RFSwitch(config-crypto-isakmp)#encryption aes
RFSwitch(config-crypto-isakmp)#hash sha
RFSwitch(config-crypto-isakmp)#authentication pre-share
RFSwitch(config-crypto-isakmp)#group 5
RFSwitch(config-crypto-isakmp)#lifetime 9496
```

d.Create and configure IPSec an transform set.

```
RFSwitch(config)#crypto ipsec transform-set TFSET ah-sha-
hmac esp-aes esp-sha-hmac
RFSwitch(config-crypto-ipsec)#mode tunnel
```

e.Create and configure a crypto map.

```
RFSwitch(config)#crypto map THIRDMAP 435 isakmp
RFSwitch(config-crypto-map)#set peer 11.1.1.10
RFSwitch(config-crypto-map)#match address 150
RFSwitch(config-crypto-map)#set transformset TFSET
RFSwitch(config-crypto-map)#set security-association
lifetime seconds 3600
```

f.Associate the crypto map with a VLAN interface.

```
RFSwitch(config)#interface vlan1
RFSwitch(config-if)#ip address 15.1.1.20/24
RFSwitch(config-if)#crypto map THIRDMAP
RFSwitch(config-if)#interface vlan2100
RFSwitch(config-if)#ip address 13.1.1.20/24
RFSwitch(config-if)#ip route 0.0.0.0/0 15.1.1.2
```

5.1.9 do

Global Configuration Commands

Runs commands from either the User Exec or Priv Exec mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
do <privilege mode commands>
```

Parameters

None

Example

```
RFSwitch(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
RFSwitch(config)#
```



NOTE: In the example above, `ping` is a PRIV EXEC command.

5.1.10 end

Global Configuration Commands

Ends the current mode and changes to the EXEC mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None.

Example

```
RFSwitch(config)#end

RFSwitch#?
Priv Exec commands:
  acknowledge    Acknowledge alarms
  archive        Manage archive files
  autoinstall    autoinstall configuration command
  cd             Change current directory
  ........................................
  ........................................
```

5.1.11 errdisable

Global Configuration Commands

Enables the timeout mechanism for the port to be enabled back after an error

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
errdisable recovery [cause bpduguard|interval <10-1000000>]
```

Parameters

recovery [cause bpduguard| interval <10-1000000>]	Enables the timeout mechanism for the port to recover after an error. • cause bpduguard – Recover from an error condition caused due to bpduguard. • interval <10-1000000> – The time interval after which a port is recovered or enabled after an error condition.

Usage Guidelines

Use `no` command with `errdisable` parameter to the disable bridge timeout mechanism for the port

Example

```
RFSwitch(config)#errdisable recovery interval 100
RFSwitch(config)#

RFSwitch(config)#errdisable recovery cause bpduguard
RFSwitch(config)#

RFSwitch(config)#no errdisable recovery cause bpduguard
RFSwitch(config)#
```

5.1.12 ftp

Global Configuration Commands

Configures the switch as an FTP server

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ftp [enable|password|rootdir]
ftp password [0 <secret>|1 <secret>|<secret>]
ftp rootdir <DIR>
```

Parameters

enable	Enables the FTP server
password [0 <secret>| 1 <secret>|<secret>]	Configures the FTP password. Set the password using one of the following options: • 0 <secret> — Password <secret> is specified unencrypted. • 1 <secret> — Password <secret> is encrypted with SHA1 algorithm. • <secret> — The password.
rootdir <DIR>	Configures the FTP root dir. Set the ROOT directory location of the FTP server using: • <DIR> — The root directory for the ftp server

Usage Guidelines

NOTE: The string size of encrypted password (option 1, Password is encrypted with SHA1 algorithm) must be exactly 40 characters.

Example

```
RFSwitch(config)#ftp enable
RFSwitch(config)#
```

5.1.13 hostname

Global Configuration Commands

Changes the system's network name

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
hostname <host-name>
```

Parameters

<host-name>	The name of the switch. This name is displayed when the switch is accessed from any network.

Example

```
RFSwitch(config)#hostname myRFSwitch
myRFSwitch(config)#
```

5.1.14 interface

Global Configuration Commands

Configures a selected interface

This command is used to enter the interface configuration mode for the specified physical *Switch Virtual Interface* (SVI) interface. If the VLANx (SVI) interface does not exist, it is automatically created.

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The interfaces mentioned below are supported in the following platforms:

- ge <index> – RFS7000 supports 4 GE's and RFS6000 supports 8 GE's
- sa <1-4> – Only supported with RFS7000
- me1 – Only supported with RFS7000 and RFS6000
- up1 – Only supported with RFS6000



NOTE: The interface mode leads to the `config-if` instance. For more information, see *Interface Instance on page 12-1*. The prompt changes from `RFSwitch(config) #` to `RFSwitch(config-if)`

Syntax (RFS7000)

```
interface [<interface-name>|ge <1-4>|me1|sa <1-4>|
  vlan <1-4094>]
```

Syntax (RFS6000)

```
interface [<interface-name>|ge <1-8>|me1|up1|vlan <1-4094>]
```

Parameters

<interface-name>	The name of the interface that is selected.
ge <1-8>	Gigabit Ethernet interface (4 for RFS7000 and 8 for RFS6000)

me1	Fast Ethernet interface
sa <1-4>	Static Aggregate interface (in RFS7000 only)
up1	WAN interface (in RFS6000 only)
vlan <1-4094>	Defines the VLAN interface

Usage Guidelines

Use the `no interface <interface-name>` to delete the specified SVI. Valid interfaces include all VLAN interfaces.

Example

```
RFSwitch(config)#interface ge 2
RFSwitch(config-if)#
```

5.1.15 ip

Global Configuration Commands

Configures a selected *Internet Protocol* (IP) component

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: Using **`access-list extended`** moves you to the **`(config-ext-nacl)`** instance. For more information, see *Chapter 14, Extended ACL Instance*.

Using **`access-list standard`** moves you to the **`(config-std-nacl)`** instance. For more information, see *Chapter 15, Standard ACL Instance*.

Using **`ip dhcp pool <pool-name>`** command to move to the **`(config-dhcp)`** instance. For additional information, see *Chapter 17, DHCP Server Instance*.

Using **`ip dhcp class <class-name>`** moves you to the **`(config-dhcpclass)`** instance. For additional information, see *Chapter 18, DHCP Class Instance*.

Syntax

```
ip [access-list|default-gateway|dhcp|domain-lookup|
  domain-name|dos|http|igmp|local|name-server|nat|route|
  routing|ssh|telnet]
ip [domain-lookup|routing]

ip access-list [standard|extended]
ip access-list extended [<100-199|<2000-2699>|<acl-name>]
ip access-list standard [<1-99>|<1300-1999>|<acl-name>]

ip default-gateway <IP>

ip dhcp [bootp|class|excluded-address|option|ping|pool]
ip dhcp bootp ignore
ip dhcp class <class-name>
ip dhcp excluded-address <IP-range-low> {<IP-range-high>}
ip dhcp option <option-name> <option-code> [ascii|ip]
```

```
ip dhcp ping timeout <1-10>
ip dhcp pool <pool-name>

ip domain-name <domain-name>

ip dos [ascend|bcast-mcast-icmp|chargen|enable|fraggle|
  ftp-bounce|invalid-protocol|option-route|router-advt|
  smurf|snork|tcp-intercept|tcp-max-incomplete|twinge]
  log [<0-8>|alerts|critical|debugging|emergencies|error|
  informational|none|notifications|warnings]

ip http [secure-server|secure-trustpoint|server]
ip http [secure-server|server]
ip http secure-trustpoint <trustpoint-name>

ip igmp-snooping {[querier|unknown-multicast-fwd|vlan]}
ip igmp-snooping {querier {[address|max-response-time|
  query-interval|timer|version]}}
ip igmp-snooping {querier {address <IP>}}
ip igmp-snooping {querier {max-response-time <1-25>}}
ip igmp-snooping {querier {query-interval <1-18000>}}
ip igmp-snooping {querier {timer expiry <60-300>}}
ip igmp-snooping {querier {version <1-3>}}
ip igmp-snooping {unknown-multicast-fwd}
ip igmp-snooping {vlan [<1-4094>|<vlan-list>]
  {mrouter|querier|unknown-multicast-fwd]}
ip igmp-snooping {vlan [<1-4094>|<vlan-list>]
  mrouter [interface <interface-list>|learn pim-dvmrp]
ip igmp-snooping {vlan [<1-4094>|<vlan-list>]
  querier {[address|max-response-time|query-interval|timer|
  version]}}
ip igmp-snooping {vlan [<1-4094>|<vlan-list>]
  unknown-multicast-fwd}

ip local pool default low-ip-address <low-IP> {high-ip-
address <high-IP>}

ip name-server <IP>

ip nat [inside|outside] [destination|source]
ip nat inside destination static <IP> <port>
  [tcp|udp] <outside-global-IP> {<outside-port>}
ip nat inside destination static <IP> {<outside-global-IP>
  <outside-port>}
ip nat inside source list <acl-name> interface [<interface-
name>|vlan <1-4094>] overload
```

```
ip nat inside source static <local-IP> <outside-global-IP>
ip nat outside destination static <IP> <outside-port>
  [tcp|udp] {<inside-global-IP> {<inside-port>}}
ip nat outside destination static <IP> {<outside-global-IP>
  <outside-port>}
ip nat outside source list <acl-name> interface [<interface-
name>|vlan <1-4094>] overload
ip nat inside source static <local-IP> <outside-global-IP>

ip route [<IP-destination-prefix> <IP-destination-prefix-
mask>|<IP-destination-prefix/Mask>] <gateway-IP>

ip ssh {[port <port>|rsa keypair-name <key-pair-name>]}

ip telnet {port <port>}
```

Parameters

ip access-list extended [<100-199|<2000-2699>|<acl-name>] ip access-list standard [<1-99>|<1300-1999>|<acl-name>]	Using the access list parameter options to enter the **`ext-nacl`** context and the **`std-nacl`** context. The prompt changes to the context entered. • For more information on extended ACL, see *Chapter 14, Extended ACL Instance*. • For more information on standard ACL, see *Chapter 15, Standard ACL Instance*.
default-gateway <IP>	Configures the IP address of the default gateway • <IP> – IP address of the next-hop router.

ip dhcp [bootp|class|excluded-address|option|ping|pool]	DHCP server configuration. • bootp ignore – Defines the BOOTP specific configuration. • ignore – Configures the DHCP server to ignore BOOTP requests. • class <class-name> – Defines a DHCP class and enters the DHCP class configuration mode. • <class-name> – The DHCP class name. • excluded-address <IP-range-low> *{<IP-range-high>}* – Prevents the DHCP server from assigning certain addresses. • <ip-range-low> – For IP range, the lower IP number. Enter this value for a single IP address. • <ip-range-high> – Optional. For IP range, the higher IP number. • option <option-name> <option-code> [ascii|ip] – Defines the DHCP server's option name. • <option-name> – Defines the name of the option. • <option-code> – Defines option code, a value in the range of 0 to 254. • ascii – Specify the option type as ascii. • ip – Specify the option type as ip. • ping timeout <1-10> – Specifies DHCP server's ping timeout in seconds. • pool <pool-name> – Configures the DHCP server's address pool <pool-name>. This opens the **`(config-dhcp)`** instance. For more information, see *Chapter 17, DHCP Server Instance*.
domain-lookup	Enables the DNS based name to address translation on the switch.
domain-name <domain-name>	Sets the domain name for the switch. • <domain-name> – The domain name string.

http [secure-server| secure-trustpoint| server]	*Hyper Text Transfer Protocol* (HTTP) configuration. • secure-server – Sets the device to start the *Secure HTTP Server* (HTTPS). • secure-trustpoint <trustpoint-name> – Sets the name of the trustpoint used for secure connection to <trustpoint-name>. • server – Sets device to start the HTTP server.
local pool default low-ip-address <low-IP> *{high-ip-address <high-IP>}*	Sets the VPN local IP pool configuration • pool default low-ip-address <low-IP> *{high-ip-address <high-IP>}* – Specifies the address range for the default group tag. • low-ip-address <low-IP> – Specifies the lowest range for IP address assignment. • high-ip-address <high-IP> – Optional. Specifies the highest range for IP address assignment.
name-server <IP>	Specifies the DNS server for the DHCP client. A maximum of 6 name servers can be configured. Servers are tried in the order entered. • <IP>– IP address of DNS server.

nat [inside|outside] [destination|source]	Defines *Network Address Translation* (NAT) configuration values. These following commands are possible for NAT • **ip nat [inside|outside] destination** static <IP> <port> [tcp|udp] <outside-global-IP> *{<outside-port>}* – Sets the parameters for translation for inside destination. • **ip nat [inside|outside] destination** static <IP> <outside-global-IP> {<outside-port>} – Sets the parameters for translation for inside destination. • inside – Indicates inside address translation. • outside – Indicates outside address translation. • destination – Indicates destination address translation. • static – Specifies local -> global address mapping. • <IP> – The local IP address. • <port> – Specifies the outside local port number. • [tcp|udp] – Specifies the protocol. • <outside-global-IP> – Specifies the outside global IP address to translate to. • <outside-port> – Optional. Specifies the outside port. Value in the range 1 to 65535. • **ip nat [inside|outside] source** list <acl-name> interface [<interface-name>|vlan <1-4094>] overload – Sets the parameters for translation for inside sources. • inside – Indicates inside address translation. • outside – Indicates outside address translation. • source – Indicates source address translation. • list <acl-name> – Specifies the ACL name <acl-name> that describes local addresses. • interface [<interface-name>|vlan <1-4094>] – The interface to apply address translation to. Specify an interface name <interface-name>, or use a VLAN ID <1-4094>. • overload – Over loads the NAT address translation.

	• **ip nat [inside|outside] source** static <outside-global-IP> <local-IP> – Sets the parameters for translation for inside sources. • inside – Indicates inside address translation. • outside – Indicates outside address translation. • source – Indicates source address translation. • static – Specifies local -> global address mapping. • <outside-global-IP> – The static global IP address to map from. • <local-IP> – The local IP address to map to.
route [<IP-destination-prefix> <IP-destination-prefix-mask>|<IP-destination-prefix/Mask>] <gateway-IP>	Adds a static route entry in the routing table. • <IP-destination-prefix>– IP destination prefix. • <IP-destination-prefix-mask> – Mask for the <IP-destination-prefix> IP. • <IP-destination-prefix/Mask> – IP destination prefix with mask. • <gateway-IP> – IP address of the next hop used to reach the destination.
routing	Turns on IP routing
ssh *{[port <port>|rsa keypair-name <key-pair-name>]}*	Sets up the Secured Shell (SSH) server • port <port> – Optional. Defines the listening port (set between 0-65536). • rsa keypair-name <key-pair-name> – Optional. Sets the RSA encryption key used for configuring RSA keypair.
telnet *{port <port>}*	Configures the Telnet server. • port <port> – Optional. Defines the listening port ID (set between 0-65535)

dos [ascend| bcast-mcast-icmp| chargen|enable|fraggle| ftp-bounce| invalid-protocol| option-route|router-advt| router-solicit|smurf| snork|tcp-intercept| tcp-max-incomplete| twinge] log [<0-8>| alerts| critical| debugging| |emergencies| errors| informational| none| notifications| warnings]	Configures the *Denial of Service* (DOS) attack parameters. • ascend – Enables Ascend DoS checks. • bcast-mcast-icmp – Detects Broadcast/Multicast Icmp traffic as attack. • chargen – Enables chargen DoS checks. • enable – Enables all DoS checks. • fraggle – Enables fraggle DoS checks. • ftp-bounce – Enables FTP bounce logs and sets the logging levels. • invalid-protocol – Enables Invalid Protocol DoS attack check and sets the logging levels for this attack. • option-route – Enables IP option route check. • router-advt – Enables ICMP router advertisement check. • router-solicit – Enables ICMP router solicit check. • smurf log – Enables smurf attack check. • snork – Enables check for packets. • tcp-intercept – Enables TCP intercept. • twinge – Enables twinge check For all the above DoS attacks, the following log options can be set. • <0-8> – Select one numerical log level. All messages with and below this severity are logged. • emergencies – System is unusable (level 0) • alerts – Immediate action needed (level 1) • critical – Critical conditions (level 2) • errors – Error conditions (level 3) • warnings – Warning conditions (level 4) • notifications – Normal but significant conditions (level 5) • informational – Informational messages (level 6) • debugging – Debugging messages (level 7) • none –Disable logging (level 8)

	• tcp -max-incomplete –Configures the maximum half-open TCP connections in the system • high <1-1000> – Sets the upper threshold value between 1 and 1000. • low <1 - 1000> – Sets the lower threshold value between 1 and1000

igmp snooping *{[querier|unknown-multicast-fwd|vlan]}*	Configures IGMP Snooping parameters. • unknown-multicast-fwd – Optional. Forwards packets from unregistered multicast servers. • querier *{[address|max-response-time|query-interval|timer|version]}}*– Configures IGMP querier. All options are optional. • address <IP> – Sets GMP querier source IP address • max-response-time <1-25> – Sets IGMP querier maximum response time in seconds • query-interval <1-18000> – Sets IGMP querier query interval • timer expiry <60-300> – Sets querier other querier time out in seconds to a value in the range 60 to 300. • version <1-3> – Sets IGMP version • vlan [<1-4094>|<vlan-list>] *{mrouter|querier|unknown-multicast-fwd]}* – Identifies the vlan to use. All options are optional. • vlan <1-4094>|<vlan-list>] – Sets the vlan to use for IGMP Snooping. • <1-4094> – A single VLAN ID. • <vlan-list> – A list of VLAN IDs. • mrouter [interface <interface> |learn pim-dvmrp] – Sets information for Multicast router. • interface <interface> – Gigabit Ethernet interfaces to be configured. <interface> can be a single interface or a list of interfaces. • learn pim-dvmrp – The multicast switch learning protocol using PIM-DVMRP protocol. • querier *{[address|max-response-time|query-interval|timer|version]}}* – Sets IGMP querier for the selected VLAN interface. • unknown-multicast-fwd – Forwards packets from unregistered multicast servers for this VLAN.

Usage Guidelines 1

1. Use the no command along with ip to undo any IP based configuration.

   ```
   [no] ip(access-list|default-gateway|dhcp|domain-lookup|
   domain-name|http|local|name-server|nat|route|routing|ssh|telnet)
   ```

2. When using the `ip access-list` parameter, enter the following contexts:

   - ext-nacl – Extended ACL. For more information, see *Chapter 14, Extended ACL Instance*
   - std-nacl – Standard ACL. For more information, see *Chapter 15, Standard ACL Instance*
   - dhcp – DHCP Server instance. For more information, see *Chapter 17, DHCP Server Instance*
   - dhcpclass – DHCP User Class instance. For more information, see *Chapter 18, DHCP Class Instance*
   - Clear the IP DHCP Binding using the *clear* command



NOTE: To delete Standard/Extended and MAC ACL use **`no access-list <access-list name>`** under the Global Config mode.

Usage Guidelines 2

To create a DHCP User Class:

Create a DHCP class

Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. `RFSwitch(config)#ip dhcp class RFSwitchDHCPclass`

```
RFSwitch(config-dhcpclass)#
```

3. Create a Pool named **`WID`**, using `(config)#` mode

   ```
   RFSwitch(config)#ip dhcp pool WID
   ```

   ```
   RFSwitch(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of only 8 CDHCP classes with a pool.

   ```
   RFSwitch(config-dhcp)#class RFSwitchDHCPclass
   ```

   ```
   RFSwitch(config-dhcp-class)#
   ```

5. The switch leads you to a new mode (config-dhcp-class). Use this mode to add an address range used with the DHCP class associated with the pool.

   ```
   RFSwitch(config-dhcp-class)#address range 11.22.33.44
   ```

Example

```
RFSwitch(config)#ip access-list extended TestACL
RFSwitch(config-ext-nacl)#

RFSwitch(config)#ip access-list standard TestStdACL
RFSwitch(config-std-nacl)#

RFSwitch(config)#ip dhcp pool TestPool
RFSwitch(config-dhcp)#

RFSwitch(config)#ip dhcp class TestDHCPclass
RFSwitch(config-dhcpclass)#
```

5.1.16 license

Global Configuration Commands

Adds a feature license

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
license <feature> <license-key>
```

Parameters

<feature>	The feature for which the license is to be added
<license-key>	The license key for the feature.

Example

```
RFSwitch(config)#show licenses
Serial Number 6283529900020
feature         license string                license value
usage
  AP
                                              48              4

RFSwitch(config)#
RFSwitch(config)#license AP <license string>
RFSwitch(config)#
```

5.1.17 line

Global Configuration Commands

Configures the terminal line

Opens the config-line mode, where you can configure the various parameters for the selected terminal.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
line [console|vty]
line console <0-0>
line vty <0-871> {<0-871>}
```

Parameters

line console <0-0>	Set the primary terminal line to 0
line vty <0-871> *{<0-871>}*	Sets the virtual terminal line to a value between 0 and 871. Optionally the last line number can also be set to a value between 0 and 871

Example

```
RFSwitch(config)# line console 0
RFSwitch(config)# line vty 0
RFSwitch(config)# line vty 0 871
RFSwitch(config)#
```

5.1.18 local

Global Configuration Commands

Sets the username and password for local user authentication

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
local username <username> password [<password>|0 <password>|
  2 <password>]
```

Parameters

username <username>	The username. A character string of up to 64 characters
password	The password for the selected username <username>. <password> is a character string of up to 21 characters. • 0 indicates that <password> is unencrypted • 2 indicates that <password> is encrypted with password-encryption secret.

Example

```
RFSwitch(config)#local username "Noble Man" password "Noble
Soul"
```

5.1.19 logging

Global Configuration Commands

Modifies message logging facilities

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
logging [aggregation-time|buffered|console|facility|
  host|monitor|on|syslog]

logging aggregation-time <1-60>

logging [buffered|console|monitor|syslog] [<0-7>|alerts|
  critical|debugging|emergencies|errors|informational|
  notifications|warnings]

logging facility [local0|local1|local2|local3|local4|local5|
  local6|local7]

logging host <IP>
loggin on
```

Parameters

aggregation-time <1-60>	Sets the number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds.

buffered [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the buffered logging level • <0-7> – Enter the logging severity level (0-7) • alerts – Immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)
console [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the console logging level.
facility [local0|local1| local2|local3|local4| local5|local6|local7]	Syslog facility in which log messages are sent. • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7
host <IP>	Configures a remote host to receive log messages. • <IP>– Remote host's IP address.

monitor [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the terminal lines logging level.
on	Enables the logging of system messages.
syslog [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the syslog servers logging level.

Example

```
RFSwitch(config)#logging on
RFSwitch(config)#logging aggregation-time 20
RFSwitch(config)#logging buffered critical
RFSwitch(config)#logging console critical
RFSwitch(config)#logging facility local6
RFSwitch(config)#logging monitor emergencies
RFSwitch(config)#logging syslog notifications
RFSwitch(config)#show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level critical
    Monitor logging: level emergencies
    Buffered logging: level critical
    Syslog logging: level notifications
     Facility: local6

Log Buffer (198 bytes):

Mar 10 15:52:00 2009: %NSM-4-IFUP: Interface vlan2 is up
Mar 10 15:52:00 2009: %NSM-4-IFUP: Interface vlan10 is up

RFSwitch(config)#
```

5.1.20 mac

Global Configuration Commands

Configures MAC access lists (goes to the MAC ACL mode)

For more information on this mode, see *Chapter 16, Extended MAC ACL Instance*.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mac access-list extended <mac-acl-name>
```

Parameters

access-list extended <mac-acl-name>	Defines the ACL configuration for the MAC address • extended <mac-acl-name>– MAC Extended ACL • <mac-acl-name> – Defines the name of the ACL

Usage Guidelines

To delete Standard/Extended and MAC ACL, use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
RFSwitch(config)#mac access-list extended Test1
RFSwitch(config-ext-macl)#
```



NOTE: When using the **`ip access-list`** parameter, enter the following contexts:

- ext-macl — extended MAC ACL. For more details see *.Extended MAC ACL Instance on page 16-1*

5.1.21 mac-address-table

Global Configuration Commands

Configures the MAC address table

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mac-address-table aging-time [0|<10-1000000>]
```

Parameters

aging-time [0|<10-1000000>]	The duration for which a learned mac address persists after the last update • 0 – Disables aging • <10-1000000> – Sets the aging time in seconds

Example

```
RFSwitch(config)#mac-address-table aging-time 100
RFSwitch(config)#
```

5.1.22 mac-name

Global Configuration Commands

Sets a name to the MAC address

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`mac-name <MAC> <mac-name>`

Parameters

<MAC> <name>	The MAC address to set a ease-of-use name for.
<mac-name>	Sets the name <name> to the MAC address <MAC> for ease of use. <name> must be configured following the DNS naming convention.

Usage Guidelines

Use `(no) mac-name` to configure the MUs name to its default. The default identity for an MU is its MAC address.

Example

```
RFSwitch(config)#mac-name 06-bc-f3-00-a0-45 ServerTecDoc
RFSwitch(config)#
RFSwitch(config)#show mac-name
Index   MAC Address        MAC Name
  1     06-BC-F3-00-A0-45  ServerTecDoc
Number of MAC names configured = 1
RFS7000(config)#
```

5.1.23 management

Global Configuration Commands

Sets management interface properties

Limits local access (through web/telnet) to management interfaces only.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
management secure
```

Parameters

secure	Limits local access (Web/Telnet etc.) to the management interface.

Example

```
RFSwitch(config)#management secure
RFSwitch(config)#
```

5.1.24 ntp

Global Configuration Commands

Configure *Network Time Protocol* (NTP) values

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ntp [access-group|authenticate|authentication-key|autokey|
broadcast|broadcastdelay|master|peer|server|trusted-key]

ntp access-group [peer|query-only|serve|serve-only]
  [<1-99>|<100-199>|<1300-1999>|<2000-2699>]

ntp authenticate

ntp authentication-key <key> md5 [0 <secret>|2
<secret>|<secret>]

ntp autokey [client-only|host]

ntp broadcast [client|destination]
ntp broadcast destination <IP> {[key <1-65534>|version
  <1-4>]}

ntp broadcastdelay <1-999999>

ntp master {<1-15>}

ntp [server|peer] <peer-name-or-IP>
ntp [server|peer] <peer-name-or-IP>
  [autokey|key|prefer|version]
ntp [server|peer] <peer-name-or-IP> autokey
  {[prefer {verson <1-4>}|version <1-4> {prefer}]}
ntp [server|peer] <peer-name-or-IP> key <1-65534> [prefer
  {verson <1-4>}|version <1-4> {prefer}]
ntp [server|peer] <peer-name-or-IP> prefer {version <1-4>}
ntp [server|peer] <peer-name-or-IP> version <1-4> {prefer}

ntp trusted-key <1-65534>
```

Parameters

access-group [peer|query-only|serve| serve-only] [<1-99>| <100-199>|<1300-1999>| <2000-2699>]	Controls NTP access. • peer – Provides full access. • query-only – Allows only control queries. • serve – Provides server and query access. • serve-only – Provides only server access. • <1-99> – Defines the standard IP access list. • <100-199> – Extended IP access list. • <1300-1999> – Standard IP access list (expanded range). • <2000-2699> – Extended IP access list (expanded range).
authenticate	Authenticates time sources.
authentication-key <key> md5 [0 <secret>| 2 <secret>|<secret>]	Defines the authentication key for trusted time sources. • md5 – Sets MD5 authentication. • 0 <secret> – Password is specified unencrypted. • 2 <secret> – Password is specified encrypted with password-encryption secret. • <secret> – Authentication key.
autokey [client-only|host]	Enables the NTP autokey authentication scheme. • client-only – The switch is a client to other trusted-hosts in the autokey group. • host – Configures the switch as a trusted host.

broadcast [client|destination]	Configures the NTP broadcast service. • client – Listens to NTP broadcasts. • destination <IP> *{[key <1-65534>|version <1-4>]}*– Configures broadcast destination address. • IP Address – Defines the destination broadcast IP address. • key <1-65536> – Optional. Sets the broadcast key number. • version <1-4> – Sets the NTP version number. **NOTE:** The switch acting as an NTP client will not associate to a broadcast IP (NTP Server) with no authentication i.e. without using symmetric key or auto-key.
broadcastdelay <1-999999>	Defines the estimated round-trip delay. • <1-999999> – Sets the round-trip delay in microseconds.
master *{<1-15>}*	Acts as a NTP master clock. • <1-15> – Optional. Sets the stratum number for the NTP master clock.
peer <peer-name-or-IP> [autokey|key|prefer| version]	Configures the NTP peer. • <peer-name-or-IP> – Sets the IP address or name of the peer. • autokey *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures an autokey peer authentication scheme. • prefer – Optional. Prefers this peer when possible. • version <1-4> – Optional. Configures the NTP version to use. • key <1-65534> *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures the autokey peer authentication key. • key <1-65535> – Sets the peer authentication key number.

	• prefer *{version <1-4>}* – Sets the preference for autokey. Optionally set the NTP version to use. • version <1-4> *{prefer}* – Sets the NTP version to use. Optionally set this peer as preferred peer.
server	Configures the NTP server. • <peer-name-or-IP> – Sets the IP address or name of the peer. • autokey *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures an autokey peer authentication scheme • prefer – Optional. Prefers this peer when possible. • version <1-4> – Configures the NTP version. • key <1-65534> *{[prefer {version <1-4>}|version <1-4> {prefer}]}* – Configures the autokey peer authentication key. • key <1-65535> – Sets the peer authentication key number. • prefer *{version <1-4>}* – Sets the preference for autokey. Optionally set the NTP version to use. • version <1-4> *{prefer}* – Sets the NTP version. Optionally set this peer as preferred peer.
trusted-key <1-65534>	Key numbers for trusted time sources. • <1-65534> – Defines the Key number.

Example

```
RFSwitch(config)#ntp peer ?
  WORD  Name/IP address of peer

RFSwitch(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>
```

```
RFSwitch(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFSwitch(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

RFSwitch(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number

RFSwitch(config)#ntp peer TestPeer autokey prefer version 3
RFSwitch(config)#

RFSwitch(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

RFSwitch(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFSwitch(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>

RFSwitch(config)#ntp peer TestPeer key 20 prefer version ?
  <1-4>  NTP version number

RFSwitch(config)#ntp peer TestPeer key 20 prefer version 2
Invalid server name "TestPeer" provided. Please enter a
valid name
RFSwitch(config)#
```

5.1.25 prompt

Global Configuration Commands

Configures and sets the systems prompt

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
prompt <prompt>
```

Parameters

<prompt>	Enter the new prompt displayed by the system. The following operational modifiers are available. • %% – Displays the % sign. • %h – Displays the host name. • %m – Displays the current configuration mode. • %n – Displays the CLI line. • %p – Displays the privilege mode prompt sign. • > - User mode prompt. • # - Priv Exec mode prompt. • (config)# - Global Config mode prompt. • %s – Displays a space. • %t – Displays a tab space. • %A – Displays date and time in ASCII format. • %D – Displays date in MM/DD/YYYY format. • %N – Displays a new line. • %T – Displays time in the hh:mm:ss format.

Example

```
RFSwitch(config)#prompt NobleMan%s%h%m%p
NobleMan RFS7000(config)#
```

5.1.26 radius-server

Global Configuration Commands

Enters the RADIUS server mode, the system prompt changes from the default config mode to the RADIUS server mode

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: **`radius-server local`** mode takes you to the RADIUS server context. For more details see *Chapter 19, Radius Server Instance*.

Syntax

```
radius-server [host|key|local|retransmit|timeout]
radius-server host <IP>
radius-server key [0 <secret>|2 <secret>|<secret>]
radius-server local
radius-server retransmit <0-100>
radius-server timeout <1-1000>
```

Parameters

host <IP>	Specifies a RADIUS server. • <IP> – Defines the IP address of RADIUS server.
key [0 <secret>| 2 <secret>|<secret>]	Sets the Encryption key shared with the RADIUS servers. • 0 <secret> – Password is specified unencrypted. • 2 <secret> – Password is encrypted with password-encryption secret. • <secret> – Text of shared key, up to 127 characters.
local	Configures local RADIUS server parameters. This takes you to a new **`config-radius-server`** context. Refer to *Chapter 19, Radius Server Instance* for more details.

retransmit <1-100>	Specifies the number of retries to active server. • <0-100> – Number of retries for a transaction (default is 3).
timeout <1-1000>	Time to wait for a RADIUS server to reply. • <1-1000> – Wait time (default 5 seconds).

Usage Guidelines

The RADIUS server host is used to configure RADIUS server details. These details are required for management user authentication if AAA authentication has been defined as RADIUS

Example

```
RFSwitch(config)#radius-server local
RFSwitch(config-radsrv)#
```

5.1.27 ratelimit

Global Configuration Commands

Configures rate limit parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ratelimit [arp|bcast|mcast|ucast] [<0-7>|alerts|critical|
debugging|emergencies|errors|informational|notifications|
warnings]
```

Parameters

ratelimit [arp|bcast|mcast|ucast] [<0-7>|alerts|critical| debugging|emergencies| errors|informational| notifications|warnings]	Sets the logging levels for ratelimit feature. • [arp|bcast|mcast|ucast] – Sets the protocol. • <0-7> – Log severity level. • alerts – immediate action needed. • critical –Critical conditions. • debugging – Debugging messages. • emergencies – System is unusable. • errors – Error conditions. • informational – Informational messages. • notifications –Normal but significant conditions. • warnings – Warning conditions.

Example

```
RFSwitch(config)# ratelimit arp log 0
RFSwitch(config)# ratelimit arp log emergencies
```

5.1.28 redundancy

Global Configuration Commands

Configures redundancy group parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
redundancy [auto-revert|auto-revert-period|
  critical-resource-ip|dhcp-server|discovery-period|
  dynamic-ap-load-balance|enable|group-id|handle-stp|
  heartbeat-period|hold-period|interface-ip|manual-revert|
  member-ip|mode]

redundancy auto-revert enable
redundancy auto-revert-period <1-1800>
redundancy critical-resource-ip <IP>
redundancy dhcp-server enable
redundancy discovery-period <10-60>

redundancy dynamic-load-balance [enable|per-ap-mu-threshold|
  schedule-interval|schedule-start-time|trigger]
redundancy dynamic-ap-load-balance enable
redundancy dynamic-ap-load-balance per-ap-mu-threshold
  <1-512>
redundancy dynamic-ap-load-balance schedule-interval <1-336>
redundancy dynamic-ap-load-balance schedule-start-time
  <HH:MM> <1-31> <1-12> <2008-2035>
redundancy dynamic-ap-load-balance trigger
  [runtime|schedule]

redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp enable
redundancy heartbeat-period <1-255>
redundancy hold-period <10-255>
redundancy interface-ip <IP>
redundancy manual-revert
redundancy member-ip <IP>
redundancy mode [primary|standby]
```

Parameters

auto-revert enable	Enables auto-revert.
auto-revert-period <1-1800>	Sets the redundancy auto-revert delay interval in minutes. The default is 5 minutes.
critical-resource-ip <ip_address>	Sets critical resource IP address. • <ip_address> – IP address of the critical resource.
dhcp-server enable	Enables the DHCP redundancy protocol.
discovery-period <10-60>	Sets the redundancy discovery interval in seconds. The default is 30 seconds.
dynamic-ap-load-balance [enable| per-ap-mu-threshold| schedule-interval| schedule-start-time| trigger]	Configures the different Dynamic AP Load Balance feature. The following are the configured options: • enable – Enables Dynamic AP Load Balance. • per-ap-mu-threshold <1-512> – Sets the threshold per-ap mu value to trigger Dynamic AP Load Balance. Set a value between 1 & 512. • schedule-interval <1-336> – Sets the time interval days to trigger Dynamic AP Load Balance. • schedule-start-time HH:MM <1-31> <1-12> <2008-2035> – Sets the scheduled start time for Dynamic AP Load Balance. • trigger [runtime|schedule] – Sets the trigger for running Dynamic AP Load Balancing. Can be either runtime or schedule.
enable	Enables the redundancy protocol.
group-id <1-65535>	Sets the cluster ID (default cluster ID is 1).
handle-stp enable	Delays the redundancy protocol state machine exec, considering STP.
heartbeat-period <1-255>	Sets the redundancy heartbeat interval.
hold-period <10-255>	Sets the redundancy hold interval.

interface-ip <IP>	Sets the redundancy interface IP address.
manual-revert	Reverts standby to non-active mode.
member-ip <IP>	Adds a member with the IP <IP> to this redundancy group.
mode [primary|standby]	Sets the mode to either primary or standby.

Example

```
RFSwitch(config)#redundancy discovery-period 20
RFSwitch(config)#

RFSwitch(config)#redundancy handle-stp enable
RFSwitch(config)#

RFSwitch(config)#redundancy heartbeat-period 20
RFSwitch(config)#

RFSwitch(config)#redundancy hold-period 25
RFSwitch(config)#

RFSwitch(config)#redundancy mode primary
RFSwitch(config)#
```

5.1.29 role

Global Configuration Commands

Configures role parameters

Opens the role configuration mode **`(confi-role)`** to enable further configuration of the role. For more information, see *Chapter 26, Role Instance*.



NOTE: Avance Security Licence must be installed for Role Based Firewall to work. Please contact customer support to purchase license for the same.

- RFS7000
- RFS6000

Syntax

```
role [<rolename>|assignment]

role <rolename> <priority>
role assignment immediate enable
```

Parameters

role <rolename> <priority>	Creates a new role with the name <rolename> and with the priority <priority> (range 1-10001). This moves to the role instance. For more information see *Chapter 26, Role Instance*.
role assignment immediate enable	Enables immediate role assignment and triggers role evaluation. This is required when a new role is added or a role is modified.

Usage Guidelines

To remove a role, use the command

```
{no} role <rolename> <priority>
```

Example

```
RFSwitch(config)# role AccMgr 10
RFSwitch(config-role)# ?
```

```
RFSwitch(config)#role assignment immediate enable

RFS7000(config)#show role

role officeuser 10
 authentication-type any
 encryption-type any
 ap-location exact "office"
 essid office
 mu-mac any
 group any

role globaluser 11
 authentication-type any
 encryption-type any
 ap-location any
 essid any
 mu-mac any
 group any

role default-role 10001
 authentication-type any
 encryption-type any
 ap-location any
 essid any
 mu-mac any
 group any
```

5.1.30 rtls

Global Configuration Commands

Configures *Real Time Location System* (RTLS) parameters

This enables the Switch to provide complete visibility to the location of assets and thereby enabling location based service.

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: `rtls` command instantiates **`(config-rtls)`** instance. For more details see *Chapter 21, RTLS Instance*. The prompt changes from `RFSwitch (config)#` to `RFSwitch (config-rtls)`

Syntax

`rtls`

Parameters

None

Example

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#
```

5.1.31 service

Global Configuration Commands

Retrieves system data (tables, log files, configuration, status and operation) for debugging and problem resolution

Supported in the following platforms:

- RFS7000
- RFS6000

To view the **`service`** command of User Exec and Priv Exec Mode, refer to *Chapter 2, service* command.

Syntax

```
service [advanced-vty|dhcp|diag|password-encryption|pm|
  prompt|radius|redundancy|set|show|terminal-length|
  watchdog]
service [advanced-vty|dhcp|

service diag [enable|limit|period|tech-support-period|
  tech-spport-url]

service password-encryption <secret>
service pm sys-restart
service prompt crash-info
service radius {restart}
service redundancy dynamic-ap-load-balance start
service set [command-history|reboot-history|upgrade-history]
```

Parameters

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server service

diag [enable|limit|period| tech-support-period| tech-support-url]	Services diagnostics configuration. • enable – Enable in service diagnostics. • limit – Displays diagnostic limit command. • period <100-30000> – Sets diagnostics period. • tech-support-period <10-10080> – Sets the tech support period. Default is 1440 minutes (1day). • tech-support-url <URL> – Sets the tech support URL to <URL>. This is used during auto generated tech support dumps.
password-encryption secret 2 <secret>	Encrypts passwords in configuration. • secret 2 <secret> – Encrypt passwords with secret phrase. • 2 – Type of encryption SHA256-AES256. • <secret> – Passphrase for encryption.
pm sys-restart	Process Monitor. • sys-restart – Enable PM to restart the system when a processes fails. **Note:** The process restart is one count less than what is configured.
prompt crash-info	Enables crash-info prompt
radius *{restart}*	Enables RADIUS server. • restart – Restarts the RADIUS server.
redundancy dynamic-ap-load-balance start	Starts Dynamic AP Load Balancing service for redundancy support.

set [command-history|reboot-history|upgrade-history]	Sets service parameters. • command-history <10-300> – Sets the number of previous commands to remember. Default 200. • reboot-history <10-100> – Sets the number of previous reboot details to remember. Default 50. • upgrade-history <10-100> – Sets the number of previous upgrade details to remember. Default 50.
show cli	Shows running system information. Shows the CLI commands for the current mode.
terminal-length <0-512>	System wide terminal length configuration.
watchdog	Enables service for watchdog.

Usage Guidelines

The **`service password-encryption`** set by the user cannot be disabled without knowing the old password. Refer the note below for more clarification.



NOTE: The **`no service password-encryption`** command used to disable the encryption, now requires the user to know the old password. The user will have to enter the old password to disable the encryption.

Earlier, using **`no service password-encryption`** disabled the encryption and `show running config` displayed the passwords as plaintext.

Now, the user has to user **`no service password-encryption <old password key>`** to disable or change the password.

Example

```
RFSwitch(config)#service dhcp
RFSwitch(config)#

RFSwitch(config)#service radius restart
RFSwitch(config)#
```

5.1.32 smtp-notification

Global Configuration Commands

Modifies SMTP notification parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
smtp-notification [authenticate|enable|password|port|prefix|
recipient|sender|smtp-server-address|user]

smtp-notification authentication enable

smtp-notification enable {traps [all|dhcp-server|
  diagnostics|miscellaneous|mobility|nsm|radius-server|
  redundancy|snmp|wireless]
smtp-notification enable traps all
smtp-notification enable traps dhcp-server
  {[dhcpServerDown|dhcpServerUp]}
smtp-notification enable traps diagnostics {[cpuLoad1Min|
  cpuLoad5Min|cpuLoad15Min|fanSpeedLow|fileDescriptors|
  ipRouteCache|packetBuffers|processMemoryUsage|ramFree|
  tempHigh|tempOver|usedKernelBuffer]}
smtp-notification enable traps miscellaneous
  {[caCertExpired|lowFsSpace|periodicHeartbeat|
  processMaxRestartsReached|savedConfigModified|
  serverCertExpired|switchEvent]}
smtp-notification enable traps mobility {[operationallyDown|
  operationallyUp|peerDown|peerUp]}
smtp-notification enable traps nsm {dhcpIPChanged}
smtp-notification enable traps radius-server
  {[radiusServerDown|radiusServerUp]}
smtp-notification enable traps redundancy{[adoptionExceeded|
  criticalResourceDown|criticalResourceUp|
  grpAuthLevelChanged|memberDown|memberMisConfigured|
  memberUp]}
smtp-notification enable traps snmp {[authenticationFail|
  coldstart|linkdown|linkup]}
smtp-notification enable traps wireless {[ap-detection|ids|
  radio|self-healing|station|wlan]}
smtp-notification enable traps wireless ap-detection
  {[externalAPDetected|externalAPRemoved]}
```

```
smtp-notification enable traps wireless ids
  {[muExcessiveEvents|radioExcessiveEvents|
  switchExcessiveEvents]}
smtp-notification enable traps wireless radio
{[adopted|unadopted|detectedRadar]}
smtp-notification enable traps wireless self-healing
  activated
smtp-notification enable traps wireless station
  {[associated|deniedAssociationAsPortCapacityReached|
  deniedAssociationOnCapability|deniedAssociationOnErr|
  deniedAssociationOnInvalidWPAWPA2IE|
  deniedAssociationOnRates|deniedAssociationOnShortPream|
  deniedAssociationOnSpectrum|deniedAssociationOnSSID|
  deniedAuthentication|disassociated|radiusAuthFailed|
  tkipCounterMeasures|vlanChanged]}
smtp-notification enable traps wireless wlan
  {[vlanUserLimitReached|webPortalUnavailable|
  webPortalUnreachable|webPortalUnconnected]}
```

```
smtp-notification password 0 <password>
smtp-notification port <1-65535>
smtp-notification prefix <smtp-prefix>
smtp-notification recipient <1-4> <recipient-address>
smtp-notification sender <sender-address>
smtp-notification smtp-server-address <IP>
smtp-notification user <username>
```

Usage Guidelines

It's recommended smtp-notification not be enabled for all traps. When smtp-notification is enabled, an email is sent to the recipients every time a trap is fired. An email is sent for each fired trap. This could potentially generate large email traffic for the recipients.

Some traps, such as Association, Disassociation, generate a large number of notifications which are then consolidated and sent as a single email every five (5) minutes.

When smtp-notification is enabled and the sender, recipient, server, and port values are not configured, then a syslog event "Incomplete Configuration" is fired every five (5) minutes till the issue is resolved.

Parameters

authenticate enable	Enables SMTP Server authentication.
enable traps [all| dhcp-server|diagnostics| miscellaneous|mobility| nsm|radius-server| redundancy|snmp |wireless]	Enables SMTP notification for traps. • all – Enables SMTP Notification for all traps. • dhcp-server [dhcpServerDown|dhcpServerUp]– Enables dhcp-server traps. • dhcpServerDown – DHCP Server down. • dhcpServerUp – DHCP Server up. • diagnostics [cpuLoad15Min|cpuLoad1Min|cpuLoad5Min| fanSpeedLow|fileDescriptors|ipRouteCache| packetBuffers|processMemoryUsage|ramFree| tempHigh|tempOver|usedKernelBuffer] – Enables diagnostics traps. • cpuLoad15Min – Average CPU load for last 15 minutes exceeds limit. • cpuLoad1Min – Average CPU load for last minute exceeds limit. • cpuLoad5Min – Average CPU load for last five minutes exceeds limit. • fanSpeedLow – Fan speed below limit. • fileDescriptors – File descriptor number exceeds limit. • ipRouteCache – IP route cache size exceeds limit. • packetBuffers – Packet buffer usage exceeds limit. • processMemoryUsage – Processor memory usage exceeds limit. • ramFree – RAM free space below limit. • tempHigh – Temperature exceeds high limit. • tempOver – Temperature exceeds critical limit. • usedKernelBuffer – Kernel buffer usage exceeds limit for some buffer size.

	• miscellaneous [caCertExpired|lowFsSpace|periodicHeartbeat| processMaxRestartsReached|savedConfigModified| serverCertExpired|switchEvent] – Enables miscellaneous traps. • caCertExpired – CA certificate has expired. • lowFsSpace – Available file system space is lower than the limit. • periodicHeartbeat – Periodic Heartbeat. • processMaxRestartsReached – Process has reached max restart. • savedConfigModified – Saved configuration has been modified. • serverCertExpired – Server certificate has expired. • switchEvent – Other switch event. • mobility – Enables mobility traps. • operationallyDown – Mobility operationally down. • operationallyUp – Mobility operationally up. • peerDown – Mobility peer down. • peerUp – Mobility peer up.

	• nsm [dhcpIPChanged] – Enables nsm traps and changes the DHCP IP. • radius-server [radiusServerDown|radiusServerUp] – Enables radius-server traps. • radiusServerDown – Radius Server is down. • radiusServerUp – Radius Server is up. • redundancy [adoptionExceeded|criticalResourceDown|criticalResourceUp|grpAuthLevelChanged|memberDown|memberMisConfigured|memberUp] – Enables redundancy traps. • adoptionExceeded – Redundancy port adoption exceeded. • criticalResourceDown – Redundancy Critical-Resource Down. • criticalResourceUp – Redundancy Critical-Resource Up. • grpAuthLevelChanged – Redundancy group Authorization Level changed. • memberDown – Redundancy member down. • memberMisConfigured – Redundancy member mis-configuration. • memberUp – Redundancy member up. • snmp [authenticationFail|coldstart|linkdown|linkup] – Enables SNMP traps. • authenticationFail – Enables authentication failure trap. • coldstart – Enables coldStart trap. • linkdown – Enables linkDown trap. • linkup – Enables linkUp trap.

	• wireless [ap-detection|ids|radio|self-healing|station| wlan] – Enables wireless traps. • ap-detection [externalAPDetected| externalAPRemoved] – Enables wireless AP detection traps. • externalAPDetected – Detects an external AP. • externalAPRemoved – Removes an external AP. • id [muExcessiveEvents|radioExcessiveEvents| switchExcessiveEvents] – Enables wireless IDS traps. • muExcessiveEvents – Excessive and Anomaly MU events. • radioExcessiveEvents – Excessive radio events. • switchExcessiveEvents – Excessive switch events. • radio [adopted|detectedRadar|unadopted] – Enables wireless radio traps. • adopted – Radio adopted. • detectedRadar – Radio detected radar. • unadopted – Radio unadopted. • self-healing [activated]– Enables self healing traps. • station [associated| deniedAssociationAsPortCapacityReached| deniedAssociationOnCapability| deniedAssociationOnErr| deniedAssociationOnInvalidWPAWPA2IE| deniedAssociationOnRates| deniedAssociationOnShortPream| deniedAssociationOnSpectrum| deniedAssociationOnSSID|deniedAuthentication| disassociated |radiusAuthFailed| tkipCounterMeasures|vlanChanged] – Enables wireless station traps.

	• associated – Wireless station associated. • deniedAssociationAsPortCapacity Reached – Wireless station denied association due to port capacity reached. • deniedAssociationOnCapability – Wireless station denied association due to unsupported capability. • deniedAssociationOnErr – Wireless station denied association due to internal error. • deniedAssociationOnInvalidWPAWPA2IE – Wireless station denied association due to invalid/ absent WPA/WPA2 IE. • deniedAssociationOnRates – Wireless station denied association due to incompatible Transmission rates. • deniedAssociationOnSSID – Wireless station denied association due to invalid SSID. • deniedAssociationOnShortPream – Wireless station denied association due to lack of short preamble support. • deniedAssociationOnSpectrum – Wireless station denied association due to lack of spectrum management capability. • deniedAuthentication – Wireless station denied 802.11 authentication. • disassociated – Wireless station disassociated. • radiusAuthFailed – Wireless station failed radius authentication. • tkipCounterMeasures – TKIP counter measures invoked. • vlanChanged – Wireless station vlan id changed.

	• wlan [vlanUserLimitReached|webPortalUnavailable| webPortalUnconnected||webPortalUnreachable] – Enables wireless wlan traps when: • vlanUserLimitReached – WLAN-VLAN user limit is reached. • webPortalUnavailable – Web portal unavailable. • webPortalUnconnected – Web portal disconnected. • webPortalUnreachable – Web portal unreachable.
password 0 <password>	SMTP Authentication Password. • 0 – Password is specified unencrypted. • <password> – Enter password up to 64 characters in length.
port <1-65535>	Enter SMTP Server TCP Port.
prefix <smtp-prefix>	Enter SMTP subject prefix up to 16 characters in length.
recipient <1-4> <recipient-address>	Enter SMTP recipient index and SMTP recipient address up to 128 characters in length.
sender <sender-address>	Enter SMTP sender address up to 128 characters in length.
smtp-server-address <IP>	Host to receive SMTP notifications. Enter IP address/ Hostname of SNMP server up to 128 characters in length.
user <username>	SMTP Authentication User. Enter username up to 64 characters in length.

Example

```
RFSwitch(config)#smtp-notification enable
RFSwitch(config)#smtp-notification enable traps dhcp-server
dhcpServerDown
RFSwitch(config)#snmp-notification recipient 1
admin@serveradmin.com
```

5.1.33 snmp-server

Global Configuration Commands

Modifies SNMP engine parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
snmp-server [community|contact|enable|engine-id|host|
  location|manager|periodic-heartbeat-interval|sysname|user]

snmp-server community <community-string> [ro|rw]
snmp-server contact <contact-person>
snmp-server enable traps {[all|dhcp-server|diagnostics|
  miscellaneous|mobility|nsm|radius-server|redundancy|snmp|
  wireless|wireless-statistics]}
snmp-server enable traps all
snmp-server enable traps dhcp-server {[dhcpServerDown|
  dhcpServerUp]}
snmp-server enable traps diagnostics {[cpuLoad1Min|
  cpuLoad5Min|cpuLoad15Min|fanSpeedLow|fileDescriptors|
  ipRouteCache|packetBuffers|processMemoryUsage|ramFree|
  tempHigh|tempOver|usedKernelBuffer]}
snmp-server enable traps miscellaneous {[caCertExpired|
  lowFsSpace|periodicHeartbeat|processMaxRestartsReached|
  savedConfigModified|serverCertExpired|switchEvent]}
snmp-server enable traps mobility {[operationallyDown|
  operationallyUp|peerDown|peerUp]}
snmp-server enable traps nsm {dhcpIPChanged}
snmp-server enable traps radius-server
  {[radiusServerDown|radiusServerUp]}
snmp-server enable traps redundancy{[adoptionExceeded|
  criticalResourceDown|criticalResourceUp|
  grpAuthLevelChanged|memberDown|memberMisConfigured|
  memberUp]}
snmp-server enable traps snmp {[authenticationFail|
  coldstart|linkdown|linkup]}
snmp-server enable traps wireless {[ap-detection|ids|
  radio|self-healing|station|wlan]}
snmp-server enable traps wireless ap-detection
  {[externalAPDetected|externalAPRemoved]}
```

```
snmp-server enable traps wireless ids
  {[muExcessiveEvents|radioExcessiveEvents|
  switchExcessiveEvents]}
snmp-server enable traps wireless radio
{[adopted|unadopted|detectedRadar]}
snmp-server enable traps wireless self-healing
  activated
snmp-server enable traps wireless station
  {[associated|deniedAssociationAsPortCapacityReached|
  deniedAssociationOnCapability|deniedAssociationOnErr|
  deniedAssociationOnInvalidWPAWPA2IE|
  deniedAssociationOnRates|deniedAssociationOnShortPream|
  deniedAssociationOnSpectrum|deniedAssociationOnSSID|
  deniedAuthentication|disassociated|radiusAuthFailed|
  tkipCounterMeasures|vlanChanged]}
snmp-server enable traps wireless wlan
  {[vlanUserLimitReached|webPortalUnavailable|
  webPortalUnreachable|webPortalUnconnected]}

snmp-server enable traps wireless-statistics [mesh|
  min-packets|mobile-unit|radio|wireless-switch|wlan]
snmp-server enable traps wireless-statistics mesh
  [avg-bit-speed-less-than|avg-retry-greater-than|
  avg-signal-less-than|gave-up-percent-greater-than|
  nu-percent-greater-than|num-mobile-units-greater-than|
  pktsps-greater-than|tput-greater-than|
  undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics min-packets
  <1-65535>
snmp-server enable traps wireless-statistics mobile-unit
  [avg-bit-speed-less-than|avg-retry-greater-than|
  avg-signal-less-than|gave-up-percent-greater-than|
  nu-percent-greater-than|pktsps-greater-than|
  tput-greater-than|undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics radio
  [avg-bit-speed-less-than|avg-retry-greater-than|
  avg-noise-level-threshold|avg-signal-less-than|
  gave-up-percent-greater-than|nu-percent-greater-than|
  num-mobile-units-greater-than|pktsps-greater-than|
  tput-greater-than|undecrypt-percent-greater-than]
snmp-server enable traps wireless-statistics wireless-switch
  [num-mobile-units-greater-than|pktsps-greater-than|
  tput-greater-than]
snmp-server enable traps wireless-statistics wlan
[avg-bit-speed-less-than|avg-retry-greater-than|
  avg-signal-less-than|gave-up-percent-greater-than|
  nu-percent-greater-than|num-mobile-units-greater-than|
```

```
  pktsps-greater-than|tput-greater-than|
  undecrypt-percent-greater-than]

snmp-server engineid [netsnmp {<word>}|text <word>]
snmp-server host <IP> [v2c|v3] {<1-65535>}
snmp-server location <location-text>
snmp-server manager [all|v2|v3]
snmp-server periodic-heartbeat-interval <interval>
snmp-server sysname

snmp-server user [snmpmanager|snmpoperator|snmptrap]
```

Parameters

community <community-string> [ro|rw]	Sets the community string and access privileges. • <community-string> – Sets the community string. • ro – Read-only access with this community string. • rw – Read-write access with this community string.
contact <contact-person>	Text for mib object sysContact. • <contact-person> – Sets the contact person for this managed node.
enable traps *{[all|dhcp-server|diagnostics|miscellaneous|mobility|nsm|radius-server|redundancy|snmp|wireless|wireless-statistics]}*	traps – Enables SNMP traps. All traps are optional. • dhcp-server – Enables dhcp-server traps. • diagnostics – Enables diagnostics traps. • miscellaneous – Enables miscellaneous traps. • mobility – Enables mobility traps. • nsm – Enables nsm traps. • radius-server – Enables RADIUS server traps. • redundancy – Enables redundancy traps. • snmp – Enables SNMP traps. • wireless – Enables wireless traps. • wireless-statistics – Enables wireless statistics traps.

enable traps dhcp-server *{[dhcpServerDown| dhcpServerUp]}*	Enables dhcp-server traps. • dhcpServerDown – DHCP server down. • dhcpServerUp – DHCP server up.
enable traps diagnostics *{[cpuLoad1Min| cpuLoad5Min| cpuLoad15Min| fanSpeedLow| fileDescriptors| ipRouteCache| packetBuffers| processMemoryUsage| ramFree|tempHigh| tempOver| usedKernelBuffer]}*	Enables diagnostics traps. • cpuLoad15Min • cpuLoad1Min • cpuLoad5Min • fanSpeedLow • fileDescriptors • ipRouteCache • packetBuffers • processMemoryUsage • ramFree • tempHigh • tempOver • usedKernelBuffer
enable traps miscellaneous *{[caCertExpired| lowFsSpace| periodicHeartbeat| processMaxRestartsReached| savedConfigModified| serverCertExpired| switchEvent]}*	Enables miscellaneous traps. • caCertExpired – CA certificate has expired. • lowFsSpace – Available file system space is lower than the limit. • periodicHeartBeat – Periodic heartbeat trap. • processMaxRestartsReached – Process has reached max restart. • savedConfigModified – Saved configuration has been modified. • serverCertExpired – Server certificate is expired. • switchEvent - Other switch event.

enable traps mobility *{[operationallyDown| operationallyUp| peerDown|peerUp]}*	Enable mobility traps. • operationallyDown – Mobility down • operationallyUp – Mobility up • peerDown – Mobility peer down • peerUp – Mobility peer up
enable traps nsm *{dhcpIPChanged}*	Enables nsm traps. • dhcpIPChanged – DHCP IP changed
enable traps radius-server *{[radiusServerDown| radiusServerUp]}*	Enables radius-server traps. • radiusServerDown – RADIUS server down • radiusServerUp – RADIUS server up
enable traps redundancy *{[adoptionExceeded| criticalResourceUp| grpAuthLevelChanged| memberDown| memberMisConfigured| memberUp| criticalResourceDown]}*	Enables redundancy traps. • adoptionExceeded – Redundancy port adoption exceeded. • grpAuthLevelChanged – Redundancy group authorization level changed. • memberDown – Redundancy member down. • memberMisConfigured – Redundancy member mis-configuration. • memberUp – Defines redundancy member as up. • criticalResourceUp – Critical resource is up. • criticalResourceDown – Critical resource is down.
enable traps snmp *{[authenticationFail| linkdown|linkup| coldstart]}*	Enables SNMP traps. • authenticationFail – Enables authentication failure trap. • coldstart – Enables coldStart trap. • linkdown – Enables linkDown trap. • linkup – Enables linkUp trap.

enable traps wireless *{[ap-detection|ids|radio|self-healing|station|wlan]}*	Enables wireless traps. • ap-detection {[externalAPDetected|externalAPRemoved]} – Enables wireless AP detection traps. • externalAPDetected – External AP detected. • externalAPRemoved – External AP detected. • ids {[muExcessiveEvents|radioExcessiveEvents|switchExcessiveEvents]} – Enables wireless IDS traps. • muExcessiveEvents – Excessive MU events. • radioExcessiveEvents – Excessive radio events. • switchExcessiveEvents – Excessive switch events. • radio {[adopted|unadopted|detectedRadar]} – Enables wireless radio traps. • adopted – Radio adopted. • detectedRadar – Radar detected. • unadopted – Radio detected radar. • self-healing activated – Enables self healing traps. • activated – Self healing activated. • station {[associated|deniedAssociationAsPortCapacityReached|deniedAssociationOnCapability|deniedAssociationOnErr|deniedAssociationOnInvalidWPAWPA2IE|deniedAssociationOnRates|deniedAssociationOnShortPream|deniedAssociationOnSpectrum|deniedAssociationOnSSID|deniedAuthentication|disassociated|radiusAuthFailed|tkipCounterMeasures|vlanChanged]} – Enables wireless station traps.

	• associated– Wireless station associated. • deniedAssociationAsPortCapacityReached – Wireless station denied association - port capacity reached. • deniedAssociationOnCapability – Wireless station denied association due to unsupported capability. • deniedAssociationOnErr – Wireless station denied association due to internal error. • deniedAssociationOnInvalidWPAWPA2IE – Wireless station denied association due to invalid/absent WPA/WPA2 IE. • deniedAssociationOnRates – Wireless station denied association due to incompatible Transmission rates. • deniedAssociationOnSSID – Wireless station denied association due to invalid SSID. • deniedAssociationOnShortPream – Wireless station denied association due to lack of short preamble support. • deniedAssociationOnSpectrum – Wireless station denied association due to lack of spectrum management capability. • deniedAuthentication – Wireless station denied 802.11 authentication. • disassociated – Wireless station disassociated. • tkipCounterMeasures – TKIP counter measures invoked. • vlanChanged – Wireless station VLAN ID has changed.

	• wlan {[vlanUserLimitReached|webPortal Unavailable|webPortalUnreachable|webPortal Unconnected]}– Enables wireless wlan traps. • vlanUserLimitReached – WALN/VLAN user limit reached. • webPortalUnavailable – Webportal is unavailable. • webPortalUnreachable – Webportal is unreachable. • webPortalUnconnected – Webportal is not connected.

snmp-server enable traps wireless-statistics [mesh| min-packets|mobile-unit| radio|wireless-switch|wlan]	Modifies wireless-stats rate traps. • mesh [avg-bit-speed-less-than| avg-retry-greater-than|avg-signal-less-than| gave-up-percent-greater-than| nu-percent-greater-than| num-mobile-units-greater-than| pktsps-greater-than|tput-greater-than| undecrypt-percent-greater-than] – Modifies mesh rate traps. • avg-bit-speed-less-than – Average bit speed in Mbps between <0.00> and <54.00>. • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00. • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00. • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00. • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00. • num-mobile-units-greater-than – Number of associated mobile-unit is <1-8192>. • pktsps-greater-than – Packets per sec is greater than 0.00 and less than or equal to 100000.00. • tput-greater-than – Throughput in Mbps is greater than 0.00 and less than or equal to 100000.00. • undecrypt-percent-greater-than – Percentage of undecryptable pkts is greater than 0.00 and less than or equal to 100.00.

	• min-packets <1-65535> – Minimum packets required for sending the trap. • <1-65535> – Defines the minimum packets for sending the trap. This can be set with a decimal number in the range of <1-65535>. • mobile-unit [avg-bit-speed-less-than| avg-retry-greater-than|avg-signal-less-than| gave-up-percent-greater-than| nu-percent-greater-than|pktsps-greater-than| tput-greater-than| undecrypt-percent-greater-than] – Modifies mobile-unit rate traps. • avg-bit-speed-less-than – Average bit speed in Mbps is between <0.00> and <54.00>. • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00. • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00. • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00. • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00. • pktsps-greater-than – Packets per sec is greater than 0.00 and less than or equal to 100000.00. • tput-greater-than – Throughput in Mbps is greater than 0.00 and less than or equal to 100000.00. • undecrypt-percent-greater-than – Percentage of undecryptable pkts is greater than 0.00 and less than or equal to 100.00.

engineid [netsnmp {<word>}| text <word>]	Sets the SNMP server engine ID. • netsnmp <word>– Sets the engine id to a hexadecimal string. • text <word> – Sets the engine id to a text string.
host <IP> [v2c|v3] {<1-65535>}	SNMP server host. • <IP> – SNMP server host IP address. • v2c <1-65535> – Use snmp version 2c. • v3 <1-65535> – Use snmp version 3.
location <location-text>	Text for mib object sysLocation.
manager [all|v2|v3]	Enables the SNMP manager. • all – Enables SNMP version v2 and v3. • v2 – Enables SNMP version v2. • v3 – Enables SNMP version v3.
periodic-heartbeat-interval <interval>	Sets periodic heartbeat trap interval. A periodic trap is sent if no other traps are sent by the switch. The default time period is 60 seconds. Set a value to between 10 and 1000 seconds.
sysname	The SNMP system name.

user [snmpmanager| snmpoperator|snmptrap]	Defines a user who can access the SNMP engine. • snmpmanager v3– Manager user • v3 [auth|encrypted] – User using v3 security model • auth md5 <password> – Sets authentication parameters for the user. • md5 – Use HMAC MD5 algorithm for authentication • <password> – The password for the user • encrypted [auth|des] – Displays privacy parameters for the user • auth md5 <password>– Displays authentication parameters for the user • des – Use CBC-DES for privacy • snmpoperator v3 – Operator user • snmptrap v3 – Trap user

Example

```
RFSwitch(config)#snmp-server community TestCommunity ro
RFSwitch(config)#

RFSwitch(config)#snmp-server contact TestManager
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps all
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps miscellaneous
lowFsSpace
RFSwitch(config)#
RFSwitch(config)#snmp-server enable traps redundancy
memberUp
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps snmp linkup
RFSwitch(config)#
```

```
RFSwitch(config)#snmp-server enable traps wireless  ap-
detection externalAPDetected
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps wireless  ids
excessiveProbes
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps wireless radio
adopted
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps wireless self-
healing activated
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps wireless station
tkipCounterMeasures
RFSwitch(config)#

RFSwitch(config)#snmp-server enable traps wireless-
statistics min-packets 120
RFSwitch(config)#

RFSwitch(config)#snmp-server location "Located at thh 5th
FLoor"
RFSwitch(config)#

RFSwitch(config)#snmp-server sysname "Gold Mine"
RFSwitch(config)#

RFSwitch(config)#snmp-server periodic-heartbeat-interval 120
RFSwitch(config)#

RFSwitch(config)#snmp-server engineid netsnmp
RFSwitch(config)#
```

5.1.34 spanning-tree

Global Configuration Commands

Configures spanning-tree commands

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
spanning-tree [mst|portfast]

spanning-tree mst [<0-15> priority <0-61440>|
cisco-interoperability [enable|disable]|configuration|
forward-time <4-30>|hello-time <1-10>|max-age <6-40>|
max-hops <7-127>]

spanning-tree portfast [bpdufilter|bpduguard] default
```

Parameters

mst [<0-15> priority <0-61440>| cisco-interoperability [enable|disable]| configuration| forward-time <4-30>| hello-time <1-10>| max-age <6-40>| max-hops <7-127>]	Enables the Multiple Spanning Tree Protocol on a bridge. • <0-15> priority <0-61440> – Set the bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default bridge priority value. • priority – Sets the bridge priority for the common instance. • <0-61440> – Defines the bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root). The default value of the priority for each instance is 32768. • cisco-interoperability [enable|disable] – Enables/ disables interoperability with Cisco's version of MSTP (incompatible with standard MSTP). • enable – Enables CISCO Interoperability. • disable – Disables CISCO Interoperability. • configuration – Multiple spanning tree configuration. This command moves to the **`(config-mst)`** instance. For more information, see *Chapter 13, Spanning tree-mst Instance*. • forward-time <4-30> – Sets the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. The default value is 15 seconds. • hello-time <1-10> – Sets the hello-time. The hello-time is the time (in seconds) after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange *Bridge Protocol Data Units* (BPDUs). A very low value leads to excessive traffic on the network, while a higher value delays the detection of a topology change. This value is used by all instances. The default value is 2 seconds.

	• max-age <6-40> – Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age must be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The permissible range for max-age is 6-40 seconds. Configure this value sufficiently high, so a frame generated by root can be propagated to the leaf nodes without exceeding the max-age. Use this command to set the max-age for a bridge. This value is used by all instances.The default value of bridge max-age is 20 seconds. • max-hops <7-127> – Specifies the maximum allowed hops for a BPDU in an MST region. This parameter is used by all MST instances. To restore the default value, use the no parameter with this command. The default maxhops in a MST region is 20.

portfast [bpdufilter|bpduguard] default	Enables the portfast feature on a bridge. It has the following options: • bpdufilter default – Use the `bpdu-filter` command to set the portfast BPDU filter for the port. Use the `no` parameter with this command to revert the port BPDU filter value to default. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFastenabled ports do not transmit or receive BPDUs. • bpduguard default – Use the `bpdu-guard` command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the `no` parameter with this command to disable BPDU Guard. When the BPDU Guard is set for a bridge, all portfast-enabled ports of the bridge that have BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. The port can be brought back up manually (using the no shutdown command), or by configuring a errdisable-timeout to enable the port after the specified interval.

Usage Guidelines

The `mst > configuration` command moves you to the *Spanning tree-mst Instance on page 13-1* Instance instance.

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

Example

```
RFSwitch(config)#spanning-tree portfast bpduguard default
RFSwitch(config)#

RFSwitch(config)#spanning-tree mst configuration
RFSwitch(config-mst)#
```

5.1.35 timezone

Global Configuration Commands

Configures switch timezone settings

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
timezone <timezone>
```

Parameters

<timezone>	Press <tab> to traverse a list of files. This displays a list of files containing timezone information.

Example

```
RFSwitch(config)#timezone
Africa/     America/    Asia/       Atlantic/   Australia/
CET
CST6CDT     EET         Etc/        Europe/     MST7MDT
Pacific/
PST8PDT     EST5EDT
RFSwitch(config)#timezone

RFSwitch(config)#timezone America/
America/Anchorage     America/Bogota        America/
Buenos_Aires  America/Caracas       America/Chicago
America/Costa_Rica    America/Denver        America/
Los_Angeles   America/Mexico_City   America/Montreal
America/New_York     America/Phoenix     America/Santiago
America/Sao_Paulo     America/St_Johns
America/Tegucigalpa   America/Thule       America/Winnipeg
America/Indianapolis

RFSwitch(config)#timezone America/Chicago
RFSwitch(config)#
```

5.1.36 traffic-shape

Global Configuration Commands

Optimizes network traffic

Supported in the following platforms:

- RFS7000



SWITCH NOTE: This command is not supported with:

- RFS6000

Syntax

```
traffic-shape [class|priority-map]
traffic-shape class <class-identifier> [max-buffers|
  max-latency|rate]
traffic-shape class <class-identifier> max-buffers
  <pri0-queue-length> <pri1-queue-length>
  <pri2-queue-length> <pri3-queue-length>
  <pri4-queue-length> <pri5-queue-length>
  <pri6-queue-length> <pri7-queue-length> red-level
  <pri0-queue-length-for-red> <pri1-queue-length-for-red>
  <pri2-queue-length-for-red> <pri3-queue-length-for-red>
  <pri4-queue-length-for-red> <pri5-queue-length-for-red>
  <pri6-queue-length-for-red> <pri7-queue-length-for-red>
traffic-shape class <class-identifier> max-buffers
  <pri0-queue-length> <pri1-queue-length>
  <pri2-queue-length> <pri3-queue-length>
  <pri4-queue-length> <pri5-queue-length>
  <pri6-queue-length> <pri7-queue-length> red-percent
  <pri0-queue-percent-for-red> <pri1-queue-percent-for-red>
  <pri2-queue-percent-for-red> <pri3-queue-percent-for-red>
  <pri4-queue-percent-for-red> <pri5-queue-percent-for-red>
  <pri6-queue-percent-for-red> <pri7-queue-percent-for-red>
traffic-shape class <class-identifier> max-latency
  <pri0-queue-latency> <pri1-queue-latency>
  <pri2-queue-latency> <pri3-queue-latency>
  <pri4-queue-latency> <pri5-queue-latency>
  <pri6-queue-latency> <pri7-queue-latency> [msec|usec]
traffic-shape class <class-identifier> rate
{[Kbps|Mbps|bps]}

traffic-shape priority-map <0-7> <0-7> <0-7> <0-7> <0-7> <0-
7> <0-7> <0-7>
```

Parameters

class <class-identifier> max-buffers ... red-level ... class <class-identifier> max-buffers ... red-percent ... class <class-identifier> max-latency ... [msec|usec] class <class-identifier> rate *{[Kbps|Mbps|bps]}*	Traffic shaping packet class. Select an identifier between 1-4. Traffic shaping also uses queues numbered 0-7. • max-buffers – Maximum traffic-shape queue length in packets. • <1-2000> – Maximum length of lowest or all priority queues. • red-level – Performs RED (random early drop) when the queue length is reached. • red-percent – Performs RED (random early drop) at a percentage of max-buffers. • max-latency – Maximum packet delay in queue. • <1-1000000> – Maximum latency of lowest or all priority queues. • [msec|usec] – Sets the time measure. • rate <1-250000000> – Traffic rate (250 Kbps-250 Mbps). • Kbps – Units of kilobits/sec. • Mbps – Units of megabits/sec. • bps – Units of bits/sec.
priority-map <0-7> <0-7> ...	Sets 802.1p to priority queue maps for all the traffic shape queues.

Example

```
RFSSwitch(config)#traffic-shape class 1 max-buffers 1000
1000 1000 1000 500 500 500 500 red-level 750 750 750 750 375
375 375 375
RFSSwitch(config)#traffic-shape class 1 max-latency 1000
1000 1000 1000 1000 1000 1000 1000 msec
RFSSwitch(config)#traffice-shape class 1 rate 100000 Kbps
RFSSwitch(config)#traffic-shape priority-map 1 2 0 7 5 3 6 4
```

```
RFSSwitch(config)#show  traffic-shape config

Traffic shaping class 1
   Rate: 10 Mbps
   Prio-|  max |    RED    | max
   rity | pkts | pkts pcnt | latency
      0 | 1000 |  750  75% | -
      1 | 1000 |  750  75% | -
      2 | 1000 |  750  75% | -
      3 | 1000 |  750  75% | -
      4 |  500 |  375  75% | -
      5 |  500 |  375  75% | -
      6 |  500 |  375  75% | -
      7 |  500 |  375  75% | -
Traffic shaping class 2
   Not configured
Traffic shaping class 3
   Not configured
Traffic shaping class 4
   Not configured
RFS7000(config)#show traffic-shape priority-map
 802.1p | Shaping priority
     0  |  1
     1  |  2
     2  |  0
     3  |  7
     4  |  5
     5  |  3
     6  |  6
     7  |  4
```

5.1.37 username

Global Configuration Commands

Establishes user name authentication

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
username <name> [access|password|privilege]
username <name> access [console|ssh|telnet|web]
username <name> password [0 <password>|1 <password>|
  <password>]
username <name> privilege [helpdesk|monitor|nwadmin|
  superuser|sysadmin|webadmin]
```

Parameters

<name>	Enter a name to authenticate the switch, the username should be between 1 and 28 characters. • access [console|ssh|telnet|web]– Sets the user access mode. • console – Only allowed from console • ssh – Only allowed from ssh • telnet – Only allowed from telnet • web – Only allowed from applet (webUI) • password [0 <password>|1 <password>|<password>] – Specifies the password for the user. • 0 – Password is specified UNENCRYPTED • 1 – Password is encrypted with SHA1 algorithm • <password> – User password • *plaintext* password length should be between 8 and 32 letters • *encrypted* password length should be 40 letters)

	• privilege [helpdesk|monitor|nwadmin|superuser| sysadmin|webadmin] – Sets user access privilege. • helpdesk – Helpdesk (troubleshooting) access • monitor – Monitor (read-only) access • nwadmin – Network (wired & wireless) admin access • superuser – Superuser (root) access • sysadmin – System (general system configuration) admin access • webadmin – Web auth (hotspot) user admin access

Example

```
RFSwitch(config)#username GoldenSwitch
RFSwitch(config)#

RFS7000(config)#username Aeyjey access console ssh telnet
web
RFS7000(config)#username JohnDoe privilege sysadmin webadmin
nwadmin
```

5.1.37.1 Encrypting a Password

To encrypt a password:

1. Enable password encryption and provide the passphrase required for encrypting the passwords.

   ```
   RFS7000(config)#service password-encryption secret 2 Symbol
   RFS7000(config)#username Jiri password Motorola
   ```

2. On completion of the above step, all the passwords, crypto keys, shared secrets etc are displayed in an encrypted format in the running/startup configuration.

   ```
   RFS7000(config)#show run
   !
   ! configuration of RFS7000 version 1.1.0.0-038R
   !
   version 1.1
   !
   !
   aaa authentication login default none
   service prompt crash-info
   ```

```
!

username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser

username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f

username Jiri password 1
399f01e13e372ba2dc02f37d869021873e60aa85
```

3. The password in the above running configuration is displayed in an encrypted format even though it was entered as plain text in Step 1.

5.1.38 vpn

Global Configuration Commands

Configures VPN authentication settings

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
vpn authentication-method [local|radius]
```

Parameters

authentication-method [local|radius]	Selects the authentication scheme. • local – Used for user based authentication. • radius – Used for RADIUS server authentication.

Usage Guidelines

Virtual Private Network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

5.1.39 wireless

Global Configuration Commands

Configures switch wireless parameters

This command moves you to the `config-wireless` instance. For more information, see *Chapter 20, Wireless Instance*.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
wireless
```

Parameters

None

Usage Guidelines

The wireless command is used to enter the config-wireless instance wherein you can configure wireless parameters. Confirm you have entered the wireless instance, as the prompt changes from the regular `RFSwitch(config)#` to `RFSwitch(config-wireless)#.`

Example

```
RFSwitch(config)#wireless
RFSwitch(config-wireless)#
```

5.1.40 wlan-acl

Global Configuration Commands

Applies an ACL on a WLAN index

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
wlan-acl <1-32> [<1-99>|<100-199>|<1300-1999>|
  <2000-2699>|<acl-name>] [in|out]
```

Parameters

`<1-32> [<1-99>|<100-199>|<1300|1999>|<2000|2699>|word] [in|out]`	WLAN number • <1-99> — IP standard access list • <100-199> — IP extended access list • <1300-1999> — IP standard access list (expanded range) • <2000-2699> — IP extended access list (expanded range) • <acl-name> — Access list name • in — Incoming packets • out — Outgoing packets

Usage Guidelines 1

Every WLAN created is mapped to an index. When an ACL is applied on a WLAN index it becomes a WLAN ACL. The following type of ACL's can be applied on a WLAN:

- IP Standard ACL
- IP Extended ACL
- MAC Extended ACL

When a packet is sent from a client to a WLAN index of an access port, it becomes an inbound traffic to the wireless LAN.

When a packet goes out of a access port, it becomes outbound traffic to the wireless LAN index. Apply an ACL to a WLAN index in outbound direction to filter traffic from both wired and wireless interfaces.

`wlan-acl` can be attached both in the inbound and outbound directions.



NOTE: Most of the Wireless LAN related configuration are performed using the *Chapter 20, Wireless Instance*.

Use `wlan-acl` (in the global configuration mode) to apply an ACL on a wireless LAN index .

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/ denied based on the ACL configuration.



NOTE: All ACLs which had WLAN index are now replaced with ones that don't have WLAN index.
In the above process, the acl "110" had two rules which got replaced by only one rule because after removal of WLAN index selector, both the rules look similar.

Follow the procedure below to manually upgrade the ACLs to the same configuration:

1. If all the rules in ACL have same WLAN index as **selector** and there are no other ACL rules, then attach the ACL to the WLAN port.

   In the above example, the ACL "**macacl**" has two rules for WLAN 14 which can be attached to WLAN port as follows:

   ```
   wlan-acl 14 macacl in
   ```

2. If the ACL has mix of rules – with different WLAN indices and without an WLAN indices, it should be grouped as follows:

   a. Create separate ACLs for all rules with a given WLAN index.

   b. Create separate ACLs for rules which do not have any WLAN index.

   To manually configure a Standard ACL, the example above has to be split into 3 ACLs.

   ```
   ip access-list standard stdacl1
   permit any rule-precedence 34

   ip access-list standard stdacl2
   permit host 10.0.0.10 rule-precedence 44
   ```

```
ip access-list standard stdacl3
deny host 30.0.0.14 rule-precedence 54

no access-list stdacl

wlan-acl 5 stdacl1 in

wlan-acl 6 stdacl2 in
```

The stdacl must be detached from the interface to which it was associated and stdacl3 must be attached to that interface.

When the user explicitly creates ACL rules with WLAN index as selector, the switch consumes that ACL without WLAN index selector. During this process a warning is raised to the user as mentioned in the example below.

```
RFSwitch(config)#access-list 14 permit any wlan 19 log
Warning : Acl rules with Wlan Index is deprecated. Wlan
index configured for the rule will be ignored. Please use
wlan-acl CLI to apply ACLs on WLAN
```

Example

The example below applies an ACL to WLAN index 200 in an inbound direction from the global config mode.

```
RFSwitch(config)#wlan-acl 2 150 in
RFSwitch(config)#
```



NOTE: A MAC access list entry to allow `arp` is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The example below applies an ACL to WLAN index 200 in outbound direction from the global config mode.

```
RFSwitch(config)#wlan-acl 2 150 out
RFSwitch(config)#
```

5.1.41 network-element-id

Global Configuration Commands

Use this command to set system's network-element-ID

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
network-element-id <element-id>
```

Parameters

<element-id>	Specifies system's network element ID

Example

```
RFSwitch(config)#network-element-id test
RFSwitch(config)#
```

5.1.42 firewall

Global Configuration Commands

Use this command to set system's network-element-ID

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
firewall [802.2-encapsulation|clamp|enable|flow|
  virtual-defrag|vlan-stacking]

firewall enable
firewall 802.2-encapsulation permit
firewall clamp [path-mtu|tcp-mss]

firewall flow timeout [icmp|other|tcp|udp]
firewall flow timeout [icmp|other|udp] <10-32400>
firewall flow timeout tcp [close-wait|established|reset|
  setup] <10-32400>

firewall virtual-defrag [enable|max-defrag-per-host|
  max-frags-per-dgram|min-1st-frag-length]
firewall virtual-defrag enable
firewall virtual-defrag max-defrag-per-host <1-32>
firewall virtual-defrag max-frags-per-dgram <2-8129>
firewall virtual-defrag min-1st-frg-length <8-1500>

firewall vlan-stacking permit
```

Parameters

enable	Enables the firewall for this switch.
802.2.-encapsulation permit	Sets 802.2 packet encapsulation. • permit – Allow 802.2 packet encapsulations which can bypass the firewall. Enabling this option is not recommended by Motorola.

clamp [path-mtu| tcp-mss]	Configures wireless firewall • clamp [path-mtu|tcp-mss] – Displays clamp value • path-mtu – Displays limit discovered path-mtu • tcp-mss – Displays limit TCP to inner path-mtu.
flow timeout [icmp|other|tcp|udp]	Configures firewall flow of packets. • timeout [icmp|other|udp] <1-32400> – Sets the timeout value for type ICMP, UDP, and Other to a value between 1 and 32400 seconds. • timeout tcp [close-wait|established|reset|setup] <10-32400> – Sets the timeout value for TCP packet types to a value between 1 and 32400 seconds. • close-wait – Configures the Closed TCP Flow timeout value • established – Configures the Established TCP Flow timeout value • reset – Configures the Reset TCP Flow timeout value • setup – Configures the Opening TCP Flow timeout value
virtual-defrag [enable| max-defrag-per-host| max-frags-per-dgram| min-1st-frag-length]	Configures IPv4 virtual defragmentation. • enable – enables IPv4 virtual defragmentation. Motorola recommends that this option be enabled. • max-defrag-per-host <1-32> – Sets the maximum active defragmentation per host to a value between 1 and 32. • max-frags-per-dgram <2-8129> – Sets the maximum allowed fragmentation per datagram to a value between 2 and 8129. • min-1st-frag-len < <8-1500> – Sets the minimum fragmentation length for the 1st fragment to a value between 8 and 1500

vlan-stacking permit	Configures 802.1q VLAN stacking. • permit – Permits 802.1q VLAN stacking that can bypass the firewall. Motorola does not recommend the use of this option.

Example

```
RFSwitch(config)#firewall clamp
RFSwitch(config)#
```

6

Crypto-isakmp Instance

The `(config-crypto-isakmp)` instance is used to configure ISAKMP policies. To enter this instance, use this command:

```
RFSwitch(config)#crypto isakmp policy <1-10000>
RFSwitch(config-crypto-isakmp)#
```

6.1 Crypto ISAKMP Config Commands

Table 6.1 summarizes **`crypto-isakmp`** commands

Table 6.1 Crypto ISAKMP Command Summary

Command	Description	Ref.
authentication	Sets the authentication scheme	*page 6-3*
clrscr	Clears the display screen	*page 6-4*
encryption	Sets the encryption algorithm	*page 6-5*
end	Ends the current mode and moves to the EXEC mode	*page 6-6*
exit	Ends the current mode and moves to the previous mode	*page 6-7*
group	Sets the Diffie-Hellman group	*page 6-8*
hash	Sets the hash algorithm	*page 6-9*
help	Provides a description of the interactive help system	*page 6-10*

Table 6.1 Crypto ISAKMP Command Summary

Command	Description	Ref.
lifetime	Sets the lifetime for the ISAKMP security association	*page 6-11*
no	Negates a command or sets its defaults	*page 6-12*
service	Defines the switch's service commands	*page 6-13*
show	Shows running system information	*page 6-15*

6.1.1 authentication

Crypto ISAKMP Config Commands

Authenticates rsa-sig and pre-share keys

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
authentication [pre-share|rsa-sig]
```

Parameters

pre-share	pre shared key
rsa-sig	rsa signature

Example

```
RFSwitch(config-crypto-isakmp)#authentication pre-share
RFSwitch(config-crypto-isakmp)#

RFSwitch(config-crypto-isakmp)#authentication rsa-sig
RFSwitch(config-crypto-isakmp)#
```

6.1.2 clrscr

Crypto ISAKMP Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFSwitch(config-crypto-isakmp)#clrscr
RFSwitch(config-crypto-isakmp)#
```

6.1.3 encryption

Crypto ISAKMP Config Commands

Configures the encryption level of the data transmitted using the `crypto-isakmp` command

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
encryption [3des|aes|aes-192|aes-256|des]
```

Parameters

3des	Triple data encryption standard
aes	Advanced data encryption standard
aes-192	Advanced data encryption standard
aes-256	Advanced data encryption standard
des	Data encryption standard

Example

```
RFSwitch(config-crypto-isakmp)#encryption 3des
RFSwitch(config-crypto-isakmp)#

RFSwitch(config-crypto-isakmp)#encryption aes-256
RFSwitch(config-crypto-isakmp)#
```

6.1.4 end

Crypto ISAKMP Config Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None.

Example

```
RFSwitch(config-crypto-isakmp))#end
RFSwitch#
```

6.1.5 exit

Crypto ISAKMP Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None.

Example

```
RFSwitch(config-crypto-isakmp)#exit
RFSwitch(config)#
```

6.1.6 group

Crypto ISAKMP Config Commands

Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy to generate keys (which is then used to create an IPSec SA)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
group [1|2|5]
```

Parameters

1	Diffie-Hellman group 1
2	Diffie-Hellman group 2
5	Diffie-Hellman group 5

Usage Guidelines

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Example

```
RFSwitch(config-crypto-isakmp)#group 5
RFSwitch(config-crypto-isakmp)#
```

6.1.7 hash

Crypto ISAKMP Config Commands

Specifies the hash algorithm used to authenticate data transmitted over the IKE SA

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
hash [md5|sha]
```

Parameters

md5	Choose the MD5 hash algorithm
sha	Choose the SHA hash algorithm

Example

```
RFSwitch(config-crypto-isakmp)#hash sha
RFSwitch(config-crypto-isakmp)#
```

6.1.8 help

Crypto ISAKMP Config Commands

Displays the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None.

Example

```
RFSwitch(config-crypto-isakmp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFSwitch(config-crypto-isakmp)#
```

6.1.9 lifetime

Crypto ISAKMP Config Commands

Specifies how long an IKE SA is valid before it expires

- RFS7000
- RFS6000

Syntax

```
lifetime <seconds>
```

Parameters

<seconds>	Specifies how many seconds an IKE SA lasts before it expires. A time stamp (in seconds) can be configured between 60 and 2147483646.

Example

```
RFSwitch(config-crypto-isakmp)#lifetime 5200
RFSwitch(config-crypto-isakmp)#
```

6.1.10 no

Crypto ISAKMP Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [authentication|encryption|group|hash|lifetime]
```

Parameters

None.

Example

```
RFSwitch(config-crypto-isakmp)#no lifetime
RFSwitch(config-crypto-isakmp)#
```

6.1.11 service

Crypto ISAKMP Config Commands

Invokes service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFSwitch(config-crypto-isakmp)#service show cli
Crypto Isakmp Config mode:
+-authentication
  +-pre-share [authentication ( rsa-sig | pre-share )]
  +-rsa-sig [authentication ( rsa-sig | pre-share )]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-encryption
  +-3des [encryption ( des | 3des | aes | aes-192 | aes-256
)]
  +-aes [encryption ( des | 3des | aes | aes-192 | aes-256
)]
  +-aes-192 [encryption ( des | 3des | aes | aes-192 | aes-
256 )]
  +-aes-256 [encryption ( des | 3des | aes | aes-192 | aes-
256 )]
  +-des [encryption ( des | 3des | aes | aes-192 | aes-256
)]
+-end [end]
+-exit [exit]
+-group
  +-1 [group (1|2|5)]
```

```
  +-2 [group (1|2|5)]
  +-5 [group (1|2|5)]
+-hash
  +-md5 [hash (sha|md5)]
...................

RFSwitch(config-crypto-isakmp)#
```

6.1.12 show

Crypto ISAKMP Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group



NOTE: For more details, see *show on page 2-37*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-crypto-isakmp)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
```

```
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
   environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notifications     Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
   traffic-shape         Display traffic shaping
  upgrade-status         Display last image upgrade status
```

```
  users                  Display information about currently
logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-crypto-isakmp)#show
```

7

Crypto-group Instance

The `(config-crypto-group)` instance configures the default group properties of the ISAKMP client.

To navigate to this instance, use the command:

```
RFSwitch(config)#crypto isakmp client configuration group
default
RFSwitch(config-crypto-group)#
```

7.1 Crypto Group Config Commands

Table 7.1 summarizes the switch **`config-crypto-group`** commands

Table 7.1 Crypto Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 7-3*
dns	Defines a primary and secondary *Domain Name Server* (DNS)	*page 7-4*
end	Ends the current mode and moves to the EXEC mode	*page 7-5*
exit	Ends the current mode and moves to the previous mode	*page 7-6*
help	Displays the interactive help system	*page 7-7*
service	Invokes service commands to troubleshoot or debug the `(config-crypto-isakmp)` instance configuration	*page 7-8*

Table 7.1 Crypto Group Command Summary

Command	Description	Ref.
show	Shows running system information	*page 7-9*
wins	Defines a *Windows Name Server* (WINS)	*page 7-12*

7.1.1 clrscr

Crypto Group Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-crypto-group)#clr
RFSwitch(config-crypto-group)#
```

7.1.2 dns

Crypto Group Config Commands

Specifies the DNS server address(es) to assign to a client

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
dns <IP>
```

<IP >	The first DNS server address to assign

Example

```
RFSwitch(config-crypto-group)#dns-server 172.1.17.1
RFSwitch(config-crypto-group)#
```

7.1.3 end

Crypto Group Config Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-crypto-group)#end
RFSwitch#
```

7.1.4 exit

Crypto Group Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-crypto-group)#exit
RFSwitch(config)#
```

7.1.5 help

Crypto Group Config Commands

Displays the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-crypto-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-crypto-group)#
```

7.1.6 service

Crypto Group Config Commands

Invokes service commands used troubleshoot or debug `(config-crypto-isakmp)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFSwitch(config-crypto-group)#service show cli
Crypto Client Config mode:
+-clrscr [clrscr]
+-dns
  +-A.B.C.D [dns A.B.C.D]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]

.............................................
.............................................
RFSwitch(config-crypto-group)#
```

7.1.7 show

Crypto Group Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group



NOTE: For more details on the show command see *show on page 2-37*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-crypto-group)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
```

```
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC Names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configures role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notification      Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
```

```
  users                  Display information about currently
logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

RFSwitch(config-crypto-group)#show
```

7.1.8 wins

Crypto Group Config Commands

Specifies the *Windows Internet Naming Service* (WINS) servers to assign to a client

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
wins <IP>
```

Parameters

<IP >	The first WINS server address to assign

Example

```
RFSwitch(config-crypto-group)#wins 128.2.11.1
RFSwitch(config-crypto-group)#
```

8

Crypto-peer Instance

The `(config-crypto-peer)` instance to configure ISAKMP peers. To enter this instance, use the command:

```
RFSwitch(config)#crypto isakmp peer [address|dn|hostname]
RFSwitch(config-crypto-peer)#
```

8.1 Crypto Peer Config Commands

Table 8.1 summarizes the **`config-crypto-peer`** commands

Table 8.1 Crypto Peer Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 8-3*
end	Ends the current mode and moves to the EXEC mode	*page 8-4*
exit	Ends the current mode and moves to the previous mode	*page 8-5*
help	Displays the system's interactive help system	*page 8-6*
no	Negates a command or sets its defaults	*page 8-7*
service	Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration	*page 8-8*
set	Sets configuration parameters	*page 8-9*

Table 8.1 Crypto Peer Command Summary (Continued)

Command	Description	Ref.
show	Displays running system	*page 8-10*

8.1.1 clrscr

Crypto Peer Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-crypto-peer)#clrscr
RFSwitch(config-crypto-peer)
```

8.1.2 end

Crypto Peer Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-crypto-peer)#end
RFSwitch#
```

8.1.3 exit

Crypto Peer Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-crypto-peer)#exit
RFSwitch(config)#
```

8.1.4 help

Crypto Peer Config Commands

Accesses the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFSwitch(config-crypto-peer)#
```

8.1.5 no

Crypto Peer Config Commands

Negates a command or sets it's defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no set aggressive-mode password
```

```
Parameters
```

See *set* command for parameters details

Example

```
RFSwitch(config-crypto-peer)#no set aggrerssive-mode
password
RFSwitch(config-crypto-peer)#
```

8.1.6 service

Crypto Peer Config Commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFSwitch(config-crypto-peer)#service show cli
Crypto Peer Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-set
    +-aggressive-mode
      +-password [no set aggressive-mode password]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
.................................
.................................

RFSwitch(config-crypto-peer)#
```

8.1.7 set

Crypto Peer Config Commands

Configures the aggressive-mode of `config-crypto-peer`

- RFS7000
- RFS6000

Syntax

```
set aggerssive-mode password [0 <password>|2 <password>|
<password>]
```

Parameters

aggressive-mode password [0 <password>|2 <password>|<password>	Defines aggressive mode attributes • password – Specifies a tunnel-password attribute • 0 <password>– Password <password> is specified unencrypted. • 2 <password> – Password <password> is specified encrypted with the password-encryption secret • <password> – The password of minimum size of 8 characters.

Example

```
RFSwitch(config-crypto-peer)#set aggressive-mode password
CheckMeIn
RFSwitch(config-crypto-peer)#
```

8.1.8 show

Crypto Peer Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group



NOTE: For more details on the show command see *show on page 2-37*

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command.

Example

```
RFSwitch(config-crypto-peer)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
```

```
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
 environment            show environmental information
  file                   Display filesystem information
 firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  role                   Configure role parameters
  redundancy             Display redundancy group parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  smtp-notifications     Display SNMP engine parameters
  sessions               Display current active open
connections
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged in users
```

```
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl

RFSwitch(config-crypto-peer)#show
```

9

Crypto-ipsec Instance

Use the `(config-crypto-ipsec)` instance to define the transform configuration for securing data (esp-3des, esp-sha-hmac etc.).

To navigate to this instance, use the command

```
RFSwitch(config)#crypto ipsec transform-set
  <transform-set-name> <encryption-type> <auth-type>
RFSwitch(config-crypto-ipsec)#
```

The transform set is assigned to a crypto map using the map's transform-set command. For more details, see *crypto-map transform set* on *page 10-12*.

9.1 Crypto IPSec Config Commands

The table below summarizes the **`config-crypto-ipsec`** commands:

Table 9.1 Crypto IPsec Command Summary

Command	Description	Ref.
show	Displays running system information	*page 9-8*
mode	Configures the IP Sec transportation mode	*page 9-6*
clrscr	Clears the display screen	*page 2-2*
end	Ends the current mode and moves to the EXEC mode	*page 9-3*
exit	Ends the current mode and moves to the previous mode	*page 9-4*
help	Describes the interactive help system	*page 9-5*

Table 9.1 Crypto IPsec Command Summary (Continued)

Command	Description	Ref.
no	Negates a command or set its defaults	*page 9-7*
service	Invokes service commands to troubleshoot or debug `(config-crypto-isakmp)` instance configurations	*page 9-10*

9.1.1 end

Crypto IPSec Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-crypto-ipsec)#end
RFSwitch#
```

9.1.2 exit

Crypto IPSec Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-crypto-ipsec)#exit
RFSwitch(config)#
```

9.1.3 help

Crypto IPSec Config Commands

Accesses the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFSwitch(config-crypto-peer)#
```

9.1.4 mode

Crypto IPSec Config Commands

Configures the IPSec mode of operation

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mode [transport|tunnel]
```

Parameters

transport	Transport mode
tunnel	Tunnel mode

Example

```
RFSwitch(config-crypto-ipsec)#mode transport
RFSwitch(config-crypto-ipsec)#
```

9.1.5 no

Crypto IPSec Config Commands

Negates a command or sets it's defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no mode
```

Parameters

mode	Sets default to tunnel mode.

Example

```
RFSwitch(config-crypto-ipsec)#no mode
RFSwitch(config-crypto-ipsec)#
```

9.1.6 show

Crypto IPSec Config Commands

Use this command to view current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-crypto-ipsec)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                    Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notifications     Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shapping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-crypto-ipsec)#show
```

9.1.7 service

Crypto IPSec Config Commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
RFS7000(config-crypto-ipsec)#service show cli
Crypto Ipsec Config mode:
+-help [help]
+-show
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-ip
    +-http
      +-secure-server [show ip http secure-server]
      +-server [show ip http server]
    +-access-group
      +-WORD [show ip access-group `WORD|ge <1-4>|me1|sa <1-
4>|vlan <1-4094>']
      +-ge
        +-<1-4> [show ip access-group `WORD|ge <1-4>|me1|sa
<1-4>|vlan <1-4094>']
      +-me1 [show ip access-group `WORD|ge <1-4>|me1|sa <1-
4>|vlan <1-4094>']
.................................
.................................

RFSwitch(config-crypto-peer)#
```

10

Crypto-map Instance

The `(config-crypto-map)` commands define a *Certificate Authority* (CA) trustpoint. This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

To navigate to this instance, use the command:

```
RFSwitch(config)#crypto map <map-name> <sequence>
  [ipsec-isakmp|ipsec-manual] {dynamic}
RFSwitch(config-crypto-map)#
```

10.1 Crypto Map Config Commands

Table 10.1 summarizes `config-crypto-map` commands:

Table 10.1 Crypto Map Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 10-3*
end	Ends the current mode and moves to the EXEC mode	*page 10-4*
exit	Ends the current mode and moves to the previous mode	*page 10-5*
help	Describes the interactive help system	*page 10-6*
match	Assigns an IP access-list to a crypto map definition	*page 10-7*
no	Negates a command or set its defaults	*page 10-9*

Table 10.1 Crypto Map Command Summary (Continued)

Command	Description	Ref.
service	Invokes service commands to troubleshoot or debug the instance configurations	*page 10-10*
set	Sets values for encryption/decryption parameters	*page 10-12*
show	Displays the running system information	*page 10-16*

10.1.1 clrscr

Crypto Map Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-crypto-map)#clrscr
RFSwitch(config-crypto-map)#
```

10.1.2 end

Crypto Map Config Commands

Ends and exits the current mode and moves to the to PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-crypto-map)#end
RFSwitch#
```

10.1.3 exit

Crypto Map Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-crypto-map)#exit
RFSwitch(config)#
```

10.1.4 help

Crypto Map Config Commands

Displays the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-crypto-map)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFSwitch(config-crypto-map)#
```

10.1.5 match

Crypto Map Config Commands

Use this command to assign an IP access-list to a crypto map definition. The access-list designates the IP packets to be encrypted by this crypto map.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map set associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists (and the crypto map entry is "respond only"), the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
match address <acl-id>
```

Parameters

address	Match the address of packets to encrypt
<acl-id>	Enter the name of the access list or ACL ID to assign to this crypto map

Usage Guidelines

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the match address command. If no ACL is configured for a crypto map, the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the OS. The source information must be the local OS, and the destination must be the peer.

Only extended access-lists can be used in crypto maps.

Example

The following entails setting up an ACL (called TestList) and assigning the new list to a crypto map (called TestMap):

```
RFSwitch(config)#ip access-list extended TestList
Configuring New Extended ACL "TestList"
(config-ext-nacl)#exit

RFSwitch(config)#crypto map TestMap 220 isakmp dynamic
RFSwitch(config-crypto-map)#

RFSwitch(config-crypto-map)#match address TestMap
RFSwitch(config-crypto-map)#
```

10.1.6 no

Crypto Map Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [match|set]
```

Parameters

Use the commands configured under this instance.

Example

```
RFSwitch(config-crypto-map)#no match address <WORD>
RFSwitch(config-crypto-map)#
```

10.1.7 service

Crypto Map Config Commands

Invokes service commands to troubleshoot or debug the `(config-crypto-peer)` instance configuration

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFSwitch(config-crypto-map)#service show cli
Crypto Map Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-match
  +-address
    +-WORD [match address WORD]
+-no
  +-match
    +-address
      +-WORD [no match address WORD]
  +-set
    +-localid [no set localid]
    +-mode [no set mode]
    +-peer
      +-A.B.C.D [no set peer (A.B.C.D |WORD)]
      +-WORD [no set peer (A.B.C.D |WORD)]
    +-pfs [no set pfs]
    +-remote-type [no set remote-type]
    +-security-association
```

```
      +-level
        +-perhost [no set security-association level
perhost]
      +-lifetime [no set security-association lifetime]
    +-session-key
      +-inbound
        +-ah [no set session-key ( inbound | outbound ) ah]
        +-esp [no set session-key ( inbound | outbound )
esp]
.............................................................
.............................................................
.............................................................
.....................
RFSwitch(config-crypto-map)#
```

10.1.8 set

Crypto Map Config Commands

Configures set parameters for the peer device

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
set [localid|mode|peer|pfs|remote-type {ipsec-l2tp|xauth}|
security-association|session-key|transform-set)

set localid [dn|hostname]<name>

set pfs [1|2|5]

set mode [aggressive|main]

set security-association [level|lifetime]
set security-association level perhost
set security-association lifetime [kilobytes|seconds]<value>

set session-key [inbound|outbound]{ah|esp}
set session-key [inbound|outbound] ah <hexkey data>
set session-key [inbound|outbound] esp <SPI>cipher<hexdata
key> authenticator <hexkey data>
set peer [ipaddress|<host name>]

set remote-type [ipsec-l2tp|xauth]
set transform-set <name>
```

Parameters

localid [dn|hostname] <name>	Sets the local identity • dn <name> – Defines the distinguished dn name • hostname <name> – Sets the hostname • <name> – The distinguished name or hostname

mode [aggressive|main]	Sets the mode of the tunnels for this Crypto Map • aggressive – Initiates aggressive mode • main – Initiates main mode
peer [ipaddress| <host name>]	Sets the IP address of the peer device. This can be set for multiple remote peers. The remote peer can be either an IP address. **Note:** In manual mode, only one remote peer can be added for a crypto map • IP address – Enter the IP address of the peer device. If not configured, it implies responder only to any peer • <host name> – Displays host name of the peer
pfs [1|2|5]	Use the *set pfs* command to choose the type of perfect forward secrecy (if any) required during IPSec negotiation of SAs for this crypto map. Use the no form of this command to require no PFS. • group 1 – IPSec is required to use the Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation • group 2 – IPSec is required to use the Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation • group 5 – IPSec is required to use Diffie-Hellman Group 5
remote-type [ipsec-l2tp| xauth]	Sets the remote VPN client type • ipsec-l2tp – Specify the remote VPN client as using IPSEC/L2TP • xauth – Specify the remote VPN client as using XAUTH with mode config

security-association [level perhost|lifetime {kilobyte|seconds}]	Defines the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map • level perhost – Specifies the security association granularity level for identities • lifetime [kilobyte|seconds] – Security an association lifetime
session-key [inbound|outbound] {ah|esp} <256-4294967295> cipher	Use the set session-key command to define the encryption and authentication keys for this crypto map • inbound [ah|esp] – Defines encryption keys for inbound traffic • outbound [ah|esp] – Defines encryption keys for outbound traffic **Note:** For information on how to create a key for authentication and encryption, refer Usage Guideline in *Global Configuration Commands* under *crypto on page 5-22*. • ah <256-4294967295> – Authentication header protocol • <256-4294967295> – *Security Parameter Index* (SPI) for the security association • esp <256-4294967295>– Encapsulating security payload protocol • <256-4294967295> cipher – Defines the security parameter index • cipher – Specify encryption/decryption key **Note:** authenticator <hex key data> – Specify an authentication key
transformset <name>	Use the set transform-set command to assign a transform-set to a crypto map

Usage Guidelines

`RFSwitch(config-crypto-map)#set peer name`

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first; then the new peer IP address can be configured.

```
RFSwitch(config-crypto-map)#set pfs
```

If left at the default setting, no *perfect forward secrecy* (PFS) is used during IPSec SA key generation. If PFS is specified, the specified Diffie-Hellman Group exchange is used for the initial (and all subsequent) key generations. This means no data linkage between prior keys and future keys.

```
RFSwitch(config-crypto-map)#set security-association lifetime
(kilobytes|seconds)
```

Values can be entered in both kilobytes and seconds. Whichever limit is reached first, ends the security association.

```
RFSwitch(config-crypto-map)#set session-key [inbound|outbound]{ah|esp}

RFSwitch(config-crypto-map)#set session-key [inbound|outbound] ah
<hexkey data>

RFSwitch(config-crypto-map)#set session-key [inbound|outbound] esp
<SPI> cipher <hexdata key> authenticator <hexkey data>
```

The inbound local SPI (security parameter index) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

They are not true ASCII strings. Therefore, a key of 3031323334353637 represents "01234567".

```
RFSwitch(config-crypto-map)#set transformset name
```

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms.

If a transform-set is not configured for a crypto map, the entry is incomplete and has no effect. For manual key crypto maps, only one transform set can be specified.

Example

```
RFSwitch(config-crypto-map)#set localid hostname TestMapHost
RFSwitch(config-crypto-map)#
```

10.1.9 show

Crypto Map Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-crypto-map)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  environment           show environmental information
  file                  Display filesystem information
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
  mac-name               Displays the configured MAC names
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy            Display redundancy group parameters
  role                  Configure role parameters
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration
parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently
logged                         in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFSwitch(config-crypto-map)#show
```

11

Crypto-trustpoint Instance

The `(config-crypto-trustpoint)` commands define a Certificate Authority (CA) trustpoint. This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

To navigate to this instance, use the command

```
RFSwitch(config)#crypto pki trustpoint <trustpoint-name>
RFSwitch(config-trustpoint)#
```

11.1 Trustpoint (PKI) Config Commands

Table 11.1 summarizes `config-crypto-trustpoint` commands:

Table 11.1 Trustpoint (PKI) Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 11-3*
company-name	Defines a company name for the trustpoint	*page 11-4*
email	Sets an e-mail ID for the trustpoint	*page 11-5*
end	Ends the current mode and moves to the EXEC mode	*page 11-6*
exit	Ends the current mode and moves to the previous mode	*page 11-7*
fqdn	Sets the domain name of the trustpoint	*page 11-8*
help	Displays the interactive help system	*page 11-9*

Table 11.1 Trustpoint (PKI) Config Command Summary

Command	Description	Ref.
ip-address	Sets an IP address for the trustpoint	*page 11-10*
no	Negates a command or sets its defaults	*page 11-11*
password	Sets the challenge password (applicable only for requests), to access the trustpoint	*page 11-12*
rsakeypair	Defines a RSA Keypair to associate with the trustpoint	*page 11-13*
service	Invokes service commands to troubleshoot or debug the `crypto pki trustpoint` instance configuration	*page 11-14*
show	Displays running system information	*page 11-15*
subject-name	The subject name is a collection of required parameters to configure a trustpoint	*page 11-17*

11.1.1 clrscr

Trustpoint (PKI) Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-trustpoint)#clrscr
RFSwitch(config-trustpoint)#
```

11.1.2 company-name

Trustpoint (PKI) Config Commands

Sets the company name (Applicable only for request)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
company-name <company-name>
```

Parameters

<company-name>	Company name (2 to 64 characters)

Example

```
RFSwitch(config-trustpoint)#company-name RetailKing
RFSwitch(config-trustpoint)#
```

11.1.3 email

Trustpoint (PKI) Config Commands

Sets the e-mail ID for the trustpoint

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
email <email>
```

Parameters

<email>	Sets email address (2 to 64 characters) for the trustpoint

Example

```
RFSwitch(config-trustpoint)#email abcTestemailID@symbol.com
RFSwitch(config-trustpoint)#
```

11.1.4 end

Trustpoint (PKI) Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-trustpoint)#end
RFSwitch#
```

11.1.5 exit

Trustpoint (PKI) Config Commands

Ends the current mode and moves to previous the mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-trustpoint)#exit
RFSwitch(config)#
```

11.1.6 fqdn

Trustpoint (PKI) Config Commands

Configures the domain name of the trustpoint (FQDN stands for Fully Qualified Domain Name)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
fqdn <domain-name>
```

Parameters

<domain-name>	The fully qualified domain name (between 9 and 64 characters long)

Example

```
RFSwitch(config-trustpoint)#fqdn RetailKing.com
RFSwitch(config-trustpoint)#
```

11.1.7 help

Trustpoint (PKI) Config Commands

Displays the systems interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-trustpoint)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-trustpoint)#
```

11.1.8 ip-address

Trustpoint (PKI) Config Commands

Sets an IP address for the trustpoint

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ip-address <IP>
```

Parameters

<IP>	Enter the IP address for the trustpoint

Example

```
RFSwitch(config-trustpoint)#ip-address 157.200.200.02
RFSwitch(config-trustpoint)#
```

11.1.9 no

Trustpoint (PKI) Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [company-name|email|fqdn|ip-address|subject-name]
```

Parameters

None.

Example

```
RFSwitch(config-trustpoint)#no ip-address
RFSwitch(config-trustpoint)#
```

11.1.10 password

Trustpoint (PKI) Config Commands

Sets the challenge password (applicable only for requests) to access the trustpoint

Syntax

```
password [0<password>|2<password>|<password>]
```

Parameters

0 <password>	Password <password> is specified as unencrypted, the password should be between 4 to 20 characters
2 <password>	Password <password> is encrypted with password-encryption secret, the string length of encrypted password should be between 44 - 64 characters
<password>	Sets the password to <password> (4 to 20 characters)

Example

```
RFSwitch(config-trustpoint)#password 0 TestPassword
RFSwitch(config-trustpoint)#
```

11.1.11 rsakeypair

Trustpoint (PKI) Config Commands

Configures a RSA Keypair to associate with the trustpoint

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rsakeypair <keypair-name>
```

Parameters

<keypair-name>	RSA Keypair Identifier

Usage Guidelines

The RSA key pair configures the switch to have *Rivest, Shamir, and Adelman* (RSA) key pairs. Thus, the switch software can maintain a different key pair for each identity certificate.

Example

```
RFSwitch(config-trustpoint)#rsakeypair were
RFSwitch(config-trustpoint)#
```

The rsakeypair name "*were*" in this example is an existing keypair value.

11.1.12 service

Trustpoint (PKI) Config Commands

Invokes service commands to troubleshoot or debug the `crypto pki trustpoint` instance configuration

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-trustpoint)#service show cli
Trustpoint Config mode:
+-clrscr [clrscr]
+-company-name
  +-WORD [company-name WORD]
+-do
  +-LINE [do LINE]
+-email
  +-WORD [email WORD]
+-end [end]
+-exit [exit]
+-fqdn
  +-WORD [fqdn WORD]
+-help [help]
+-ip-address
  +-A.B.C.D [ip-address A.B.C.D]
+-no
  +-company-name [no company-name]
  +-email [no email]
  +-fqdn [no fqdn]
  +-ip-address [no ip-address]
  +-subject-name [no subject-name]
.....................................................
.....................................................
.....................................................
RFSwitch(config-trustpoint)#
```

11.1.13 show

Trustpoint (PKI) Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-trustpoint)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
 environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
smtp-notification        Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  traffic-shape         Display traffic shaping
  timezone               Display timezone
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged                          in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-crypto-map)#show
```

11.1.14 subject-name

Trustpoint (PKI) Config Commands

Creates a subject name to configure a trustpoint (the subject name is a collection of required parameters to configure a trustpoint)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
subject-name <name> <country> <state> <city> <org>
<org-unit>
```

Parameters

<name>	Name of this set of parameters for configuring trust points
<country>	The 2 character ISO country code
<state>	The state in the country (2 to 128 characters)
<city>	The city name (2 to 128 characters)
<org>	The organization name (2 to 128 characters)
<org-unit>	The name of the unit in the organization (2 to 128 characters)

Example

```
RFSwitch(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

RFSwitch(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

RFSwitch(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

RFSwitch(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )
```

```
RFSwitch(config-trustpoint)#subject-name TestPool US OH PB
SYMBOL ?
  WORD  Organization Unit( 2 to 64 characters )

RFSwitch(config-trustpoint)#subject-name TestPool US OH PB
SYMBOL WID ?
  <cr>

RFSwitch(config-trustpoint)#subject-name TestPool US OH PB
SYMBOL WID
RFSwitch(config-trustpoint)#
```

12

Interface Instance

Use the `(config-if)` instance to configure the interfaces – Ethernet, VLAN and tunnel associated with the switch.

To switch to this mode, use the command:

```
RFSwitch(config)#interface [<interface-name>|ge <1-4>|me1|
  sa <1-4>|vlan <1-4094>
RFSwitch(config-if)#
```

12.1 Interface Config Commands

Table 12.1 summarizes the `(config-if)` commands:

Table 12.1 Interface Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 12-3*
crypto	Defines the encryption module	*page 12-4*
description	Creates an interface specific description	*page 12-5*
duplex	Sets the duplex mode used by the interface	*page 12-6*
end	Ends the current mode and moves to the EXEC mode	*page 12-7*
exit	Ends the current mode and moves to the previous mode	*page 12-8*
help	Displays the interactive help system	*page 12-9*

Table 12.1 Interface Config Command Summary (Continued)

Command	Description	Ref.
ip	Sets the IP address for the assigned ethernet, VLAN or tunnel	*page 12-10*
mac	Applies a MAC access list to a gigabit ethernet interface	*page 12-13*
management	Sets the selected interface as the management interface	*page 12-14*
no	Negates a command or sets its defaults	*page 12-15*
port-channel	Configures the load-balancing criteria of an aggregated port	*page 12-16*
power	PoE (Power Over Ethernet) commands used to configure PoE power limit and priority for a port	*page 12-19*
service	Invokes service commands to troubleshoot or debug the **`(config-if)`** instance configurations	*page 12-21*
show	Displays running system information	*page 12-22*
shutdown	Shuts down a selected interface	*page 12-24*
spanning-tree	Disables the selected interface. The interface is administratively enabled unless explicitly disabled using this command	*page 12-25*
speed	Specifies the speed of a fast-ethernet (10/100) or a gigabit ethernet port (10/100/1000)	*page 12-28*
static-channel-group	Configures static channel commands	*page 12-29*
storm-control	Sets broadcast rate-limit value	*page 12-32*
switchport	Sets switching mode characteristics	*page 12-30*

12.1.1 clrscr

Interface Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-if)#clrscr
RFSwitch(config-if)#
```

12.1.2 crypto

Interface Config Commands

Sets the encryption module to use for this interface

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
crypto map <map-tag>
```

Parameters

map <map-tag>	Assigns a Crypto Map • <map-tag> – Crypto Map tag

Usage Guidelines

At any given instance you can add one crypto mapset to an single interface. The switch does not allow the same cryptomap set to be attached to multiple interfaces.

12.1.3 description

Interface Config Commands

Creates an interface specific description

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
description <description>
```

Parameters

<description>	Defines the characters describing this interface

Example

```
RFSwitch(config-if)#description "interface for RetailKing"
RFSwitch(config-if)#
```

12.1.4 duplex

Interface Config Commands

Specifies the duplex mode for the interface



NOTE:

- Duplexity can only be set for an Ethernet Interface. Enter the `(config-if)` instance using the `eth` parameter of the `interface` mode
- The duplex cannot be set until the speed is set to a non-auto value

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
duplex [auto|full|half]
```

Parameters

auto	Sets the ports duplexity automatically. The port automatically detects whether it should run in full or half-duplex mode
full	Sets the port in full-duplex mode
half	Sets the port in half-duplex mode

Usage Guidelines

The duplex defines the communication used by the port. The switch (by default) is set in the auto duplex mode. In auto mode, the duplex is selected based on connected network hardware.

12.1.5 end

Interface Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-if)#end
RFSwitch#
```

12.1.6 exit

Interface Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-if)#exit
RFSwitch(config)#
```

12.1.7 help

Interface Config Commands

Displays the system's interactive help

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-if)#
```

12.1.8 ip

Interface Config Commands

Sets the IP address for the assigned Gigabit Ethernet interface (GE), Fast Ethernet interface (ME), LAN interface (UP), Ethernet interface (ETH), Static Aggregate interface (SA) or VLAN Interface

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ip [access-group|address|arp|dhcp|helper-address|nat]
ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|WORD in]
ip arp [rate-limit|trust]
ip dhcp trust
ip address [<IP/Mask> {secondary}|dhcp]
ip helper-address <IP> [<interface>|ge <1-4>|me1|
sa <1-4>|vlan <1-4094>]
ip nat [inside|outside]
```

Parameters

access-group [<1-99>| <100-199>| <1300-1999>| <2000-2699>]	Defines the access group • <1-99> – Sets the IP standard access list • <100-199> – Sets the IP extended access list • <1300-1999> – Sets the IP standard access list (expanded range) • <2000-2699> – Sets the IP extended access list (expanded range) • WORD in – Defines the access list name • in – Sets incoming packets

ip address [<IP Mask> {secondary}|dhcp]	Sets a static IP address and network mask for a Layer 3 SVI (*Switch Virtual Interface*) • <IP/ Mask> {secondary} – Sets the IP address (10.0.0.1/8) • secondary – Defines an optional secondary IP address • dhcp – Uses a DHCP Client to obtain an IP address for the interface (this enables DHCP on a Layer 3 SVI)
helper-address <IP> [<interface>|ge <1-4>|me1| sa <1-4>|vlan <1-4094>]	Forwards DHCP and BOOTP packets • <IP> [<interface>|ge|me1|sa|vlan]– Defines the IP to which DHCP and BOOTP packets are forwarded • <interface> – Interface name • ge[<1-4>] – Gigabit Ethernet interface index • sa[<1-4>] – Static Aggregate interface index • vlan[<1-4094>] – VID
nat [inside|outside]	Sets *Network Address Translation* (NAT) parameters • inside – Inside interface • outside – Outside interface
arp [rate-limit <1-1000000>| trust]	Sets arp for the packets • rate-limit <1-1000000> – Displays the allowed rate in packets per second • trust – Displays trust state for arp responses coming in this interface
dhcp trust	Sets dhcp trust state for dhcp responses coming in this interface

Usage Guidelines

IPv4 commands are not allowed on a L2 interface. Use the `ip access-group` command to attach an access list to an interface. Use the `no ip access-group` command to remove the access list from the interface

Use `mac access-group` to attach a MAC access list to an interface

Use the `{no} ip [options]` command to undo IP based interface configurations

Example

```
RFSwitch(config-if)#ip access-group 110 in
RFSwitch(config-if)#

RFSwitch(config-if)#ip address 192.168.234.1/24
RFSwitch(config-if)#
```

12.1.8.1 Creating Helper Address using DHCP Server

Follow the steps below to create a helper address on VLAN 2000 for using a DHCP server on VLAN 1000:

```
RFSwitch(config)#interface vlan 1000
RFSwitch(config-if)#ip address 172.168.100.1/24

RFSwitch(config-if)#interface vlan 2000
RFSwitch(config-if)#ip address 172.168.200.1/24
RFSwitch(config-if)#ip helper-address 172.168.100.10 vlan
1000
RFSwitch(config-if)#
```

12.1.8.2 Configuring a Static NAT Source Translation

The example below displays static NAT source translation:

```
RFSwitch(config)#interface vlan 1000
RFSwitch(config-if)#ip nat inside

RFSwitch(config-if)#interface vlan 2000
RFSwitch(config-if)#ip nat outside

RFSwitch(config)#ip nat inside source static 172.168.200.10
157.235.205.57
RFSwitch(config)#
```

12.1.9 mac

Interface Config Commands

Applies a MAC access list (ACL) to Gigabit Ethernet interface

NOTE: The access list cannot be applied on a management interface (me1).

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mac access-group <acl-name> in
```

Parameters

access-group <acl-name>	Sets the MAC access groups ACL • <acl-name> – Sets ACL name • in – Applies the ACL to ingress packets

Example

```
RFSwitch(config-if)#mac access-group Ark200 in
RFSwitch(config-if)#
```

12.1.10 management

Interface Config Commands

Sets the selected interface as management interface. It can only be used on a VLANx interface. The TFTP/FTP server providing the switch its config file at startup must be accessible via this interface.

VLAN 1 is the default management interface for the switch.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`management`

Parameters

None

Usage Guidelines

The management privilege can be set only on a L3 interface. Use this command along with the `(config) management secure` in the config mode. This ensure management access is restricted to the management VLAN only

Refer to *management on page 5-67* for `management` configuration.

Example

```
RFSwitch(config)#interface vlan 1000
RFSwitch(config-if)#management
RFSwitch(config-if)#
```

12.1.11 no

Interface Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands are not supported on RFS6000:

- port-channel
- static-channel-group



SWITCH NOTE: The following command is not supported on RFS7000:

- power

Syntax

```
no [crypto|description|duplex|ip|mac|port-channel|
shutdown|spanning-tree|speed|static-channel-group|
storm-control|switchport]
```

Parameters

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFSwitch(config-if)#no duplex
RFSwitch(config-if)#
```

12.1.12 port-channel

Interface Config Commands

Selects the load-balance criteria of an aggregated port

Supported in the following platforms:

- RFS7000



SWITCH NOTE: RFS6000 does not support this command.

Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

Parameters

load-balance [src-dst-ip|src-dst-mac]	Sets load-balancing for port channel • src-dst-ip – Defines the Source and Destination IP address based on the current load balancing • src-dst-mac – Sets the Source and Destination MAC address based on the load balancing

Usage Guidelines

Use this command to configure and set load balance on the aggregated port using `(config-if) static-channel-group`.

Example

The following example creates a channel group 1, with interface ge1 and ge 2:

```
RFSwitch(config)#interface ge1
RFSwitch(config-if)#static-channel-group 1

RFSwitch(config)#interface ge2
RFSwitch(config-if)#static-channel-group 1
```

The following example defines the load balance based on the IP or MAC address:

```
RFSwitch(config)#interface sa1
RFSwitch(config-if)#port-channel load-balance src--dst-ip
RFSwitch(config-if)#
```

12.1.12.1 Configuring a Port Aggregation

Use `static-channel-group` and `port-channel` for configuring port aggregation. Follow the steps below to configure port aggregation:

1. Create a static channel group for port aggregation and associate an interface with it.

   ```
   RFSwitch(config)#interface ge 1
   RFSwitch(config-if)#static-channel-group 1
   ```

2. Execute `show static-channel-group` and ensure the virtual static aggregation sa 1 has been created and associated with `ge 1.`

3. Select the other interface required for port aggregation and associate the static channel group to it.

   ```
   RFSwitch(config)#interface ge 2
   RFSwitch(config-if)#static-channel-group 1
   ```

4. Execute `show static-channel-group` and ensure the virtual static aggregation sa 1 has been created and associated with `ge 2.`
   Both ge 1 and ge 2 are now aggregated and ready for use.

5. Use the `port-channel` command to select the criteria used to determine which link is selected for a given packet. The port-channel selection is based on either source-destination IP or source destination MAC

   ```
   RFS7000(config-if)#port-channel load-balance src-dst-ip
   RFS7000(config-if)#
   ```

   The default port-channel criteria is based on source-destination IP. The port channel (when configured with `src-dst-ip)` does not show up in the running-config. Hence, this mode is preferred over `src-dst-mac.`



NOTE: When a port (GE) is aggregated into a *Static Aggregation* (SA), it temporarily takes on the port configuration of the SA.

For example, If GE 1 (previously configured as trunk vlan 1-10) and GE 2 (previously configured as trunk vlan 11-20) are now aggregated as SA 1 and SA 1 is configured as trunk vlan 100-200, then SA 1's configuration applies to both GE 1 and GE 2. This new configuration like VLAN, speed, duplex, MST is now applicable on the ports as long as they are part of the SA. The ports revert back to the original configuration once they are removed from the SA.

How src-dst-mac mode works

When the switch sends a packet out of a SA, it selects the egress port as a function of the packet's source MAC, destination MAC, and the set of ports in the SA which are running. It XORs the bottom bits of the two MACs and indexes it into a table of the running ports.

How src-dst-ip mode works

When the switch sends an IP packet, the egress port is chosen as a function of the packet's source IP, destination IP and the set of running ports. It XORs the bottom byte of the two IP addresses and indexes then into the same table of running ports that `src-dst-mac` mode uses.

If the packet is NOT an IP packet, it uses the same calculation as src-dst-mac mode.

Why is src-dst-ip mode preferred

src-dst-ip mode distributes packets better when most packets, going through the gateway, are IP packets. In the presence of an IP gateway, the IP packets forwarded from one MU to hosts that is beyond the gateway all have the same MAC pair <MU MAC, Gateway MAC> no matter what host the MU is accessing.

But in src-dst-mac balancing, the same link is selected always.

12.1.13 power

Interface Config Commands

Invokes PoE commands to configure PoE power limit and priority for a port. By default the value for a GE port is set to low. Power is applied in order of priority, power overlaods are removed in reverse order of priority.

Supported in the following platforms:

- RFS6000



SWITCH NOTE: This command is not supported with:

- RFS7000

Syntax

```
power [limit <0-30>|priority {critical|high|low}]
```

Parameters

limit <0-30>	Sets the power limit on the given port to the stated power in Watts. Select the power limit value between 0-30 (Watts). It actually limits to 29.7W
priority [critical|high|low]	Sets PoE priority for port • critical – Sets the PoE priority as critical priority • high – Sets the PoE priority as high priority • low – Sets the PoE priority as low priority

Usage Guidelines

Use `[no] power` to rollback the PoE configurations and set back the default configuration

Example

```
RFSwitch(config)#interface ge1
RFSwitch(config-if)#no power
RFSwitch(config-if)#exit
RFSwitch(config)#interface ge2
RFSwitch(config-if)#power limit 14
RFSwitch(config-if)#exit
```

```
RFSwitch(config)#interface ge3
RFSwitch(config-if)#power priority critical
RFSwitch(config-if)#exit
RFSwitch(config)#show power configuration
Power usage trap at 80% of max power (148 of 185 Watts)
 port  Priority    Power limit  Enabled
  ge1  high        29.7W         no
  ge2  high        14.0W        yes
  ge3  crit        29.7W        yes
  ge4  high        29.7W        yes
  ge5  high        29.7W        yes
  ge6  high        29.7W        yes
  ge7  high        29.7W        yes
  ge8  high        29.7W        yes
 POE firmware version 01f6 build 4
RFSwitch(config)#
```

12.1.14 service

Interface Config Commands

Invokes service commands to troubleshoot or debug the `(config-if)` instance configuration.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFSwitch(config-if)#service show cli
Interface Config mode:
+-clrscr [clrscr]
+-crypto
  +-map
    +-WORD [crypto map WORD]
+-description
  +-LINE [description LINE]
+-do
  +-LINE [do LINE]
+-duplex
  +-auto [duplex (half|full|auto)]
  +-full [duplex (half|full|auto)]
  +-half [duplex (half|full|auto)]
+-end [end]
+-exit [exit]
+-help [help]
+-ip
  +-access-group
    +-<1-99>
      +-in [ip access-group (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD) (in)]
    +-<100-199>
RFSwitch(config-if)#
```

12.1.15 show

Interface Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-if)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
   environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  smtp-notification      Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged                          in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-if)#show
```

12.1.16 shutdown

Interface Config Commands

Disables the selected interface, the interface is administratively enabled unless explicitly disabled using this command

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
shutdown
```

Parameters

None

Example

```
RFSwitch(config-if)#shutdown
RFSwitch(config-if)#
```

12.1.17 spanning-tree

Interface Config Commands

Configures spanning tree parameters

Displays current system information running on the switch.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
spanning-tree [bpdufilter|bpduguard|edgeport|force-version|
guard|link-type|mst|portfast]
spanning-tree bpdufilter [enable|disable]
spanning-tree bpduguard [enable|disable]
spanning-tree [edgeport|portfast]
spanning-tree force-version <1-3>
spanning-tree guard root
spanning-tree link-type [point-to-point|shared]
spanning-tree mst [<1-15|port-cisco]
spanning-tree mst 1 [cost <>|port-priority <>]
spanning-tree mst port-cisco [enable|disable]
```

Parameters

bpdufilter [disable|enable]	Use this command to set a portfast BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFastenabled ports do not transmit or receive BPDUs.

bpduguard [disable|enable]	Use this command to enable or disable the BPDU guard feature on a port. Use the no parameter with this command to set the BPDU guard feature to default values. When the BPDU guard is set for a bridge, all portfast-enabled ports that have the BPDU-guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edgeport
force-version <0-3>	Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • 0 – STP • 1 – Not supported • 2 – RSTP • 3 – MSTP The default value for forcing the version is MSTP
guard root	Enables the Root Guard feature for the port. The root guard disables the reception of superior BPDUs. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the no parameter with this command to disable the root guard feature.
link-type [point-to-point|shared]	Enables or disables point-to-point or shared link types • point-to-point – Enables rapid transition • shared – Disables rapid transition

mst [<0-15> [cost <1-200000000>| port-priority <0-240>]| port-cisco-interoperability [disable|enable]]	Configures MST values on a spanning tree • <0-15> [cost <1-200000000>|port-priority <0-240>] – Defines the Instance ID • cost <1-200000000> – Defines the path cost for a port • port-priority <0-240> – Defines the port priority for a bridge • port-cisco-interoperability [disable|enable] – Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP). • enable – Enables CISCO Interoperability • disable – Disables CISCO Interoperability - The default value is disabled
portfast	Enables rapid transitions

Example

```
RFSwitch(config-if)#spanning-tree edgeport
RFSwitch(config-if)#

RFSwitch(config-if)#spanning-tree guard root
RFSwitch(config-if)#

RFSwitch(config-if)#spanning-tree link-type point-to-point
RFSwitch(config-if)#
```

12.1.18 speed

Interface Config Commands

Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)

Displays current system information running on the switch.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
speed [10|100|1000|auto]
```

Parameters]

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	Port automatically detects the speed it should run based on the port at the other end of the link.Autonegotiation is a requirement for using 1000BASE-T[3] according to the standard.

Usage Guidelines

Set the interface speed to auto to detect and use the fastest speed available. Speed detection is based on connected network hardware.

Example

```
RFSwitch(config-if)#speed auto
RFSwitch(config-if)#
```

12.1.19 static-channel-group

Interface Config Commands

Adds an interface to a static channel group

Displays current system information running on the switch.

Supported in the following platforms:

- RFS7000



SWITCH NOTE: RFS6000 does not support this command

Syntax

```
static-channel-group <1-4>
```

Parameters

<1-4>	Sets a static channel group to associate the link with

Usage Guidelines

This command aggregates individual giga ports into a single aggregate link to provide greater bandwidth. The static channel group is used to provide additional bandwidth in multiples of 1Gbps on the switch. All MAC layer and higher protocols see only the static channel group (aggregate link) rather than the individual ports that comprise it.

Example

```
RFSwitch(config-if)#static-channel-group 2
RFSwitch(config-if)#
```

12.1.20 switchport

Interface Config Commands

Sets switching mode characteristics for the selected interface.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
switchport [access|mode|trunk]
switchport access vlan <1-4094>
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [add|none|remove] <vlan-id>
switchport trunk native [tagged|vlan<1-4094>]
```

Parameters

access vlan <1-4094>	Configures the access vlan of an access-mode port • vlan <1-4094> – Sets the vlan when interface is in access mode
mode [access|trunk]	Sets the mode of the interface to access or trunk mode (can only be used on physical (layer2) interfaces) • access – If `access` mode is selected, the access vlan is automatically set to vlan1. In this mode, only untagged packets in the access vlan (vlan1) are accepted on this port. All tagged packets are discarded. • trunk – If `trunk` mode is selected, tagged vlan packets VLANs are accepted. The native vlan is automatically set to VLAN1. Untagged packets are placed in the native vlan by the switch. Outgoing packets in the native vlan are sent untagged. `trunk` is the default mode for both ports

trunk [allowed |native]	Sets the trunking mode characteristics • allowed vlan – Configures trunk characteristics when the port is in trunk-mode • vlan [add|none|remove] – Sets allowed vlans • none – Allows no vlans to Xmit/Rx through the Layer2 interface • add – Adds vlans to the current list • remove – Removes vlans from the current list • <vlan-id> – vlan-ids added or removed. Can be either a range of vlans (55-60) or a list of comma separated vlan-ids (35, 41 etc.) • native [tagged|vlan <1-4094>] – Configures the native VLAN ID of the trunk-mode port • tagged – Tags the native vlan • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode

Usage Guidelines

Interfaces ge1-ge4 can be configured as trunk or in access mode. An interface (when configured as trunk) allows packets (from the given list of vlans) to be added to the trunk. An interface configured as "*access*" allows packets only from native vlans

Use the `[no] switchport (access|mode|trunk)`to undo switchport configurations

Example

```
RFSwitch(config-if)#switchport mode access
RFSwitch(config-if)#
```

12.1.21 storm-control

Interface config commands

Sets storm-control for broadcasting

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
storm-control [bcast|mcast|ucast] rate-limit <1-1000000>
```

Parameters

bcast rate-limit <1-1000000>	Configures storm-control of broadcast packets. • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per second
mcast rate-limit <1-1000000>	Configures storm-control of multicast packets. • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per sec ond
ucast rate-limit <1-1000000>	Configures storm-control of unicast packets • rate-limit <1-1000000> – Performs packet rate limiting • <1-1000000> – Displays allowed rate in packets per sec ond

Example

```
RFSwitch(config-if)#storm-control bcast ratelimit 88
RFSwitch(config-if)#
RFSwitch(config-if)#storm-control mcast ratelimit 88
RFSwitch(config-if)#
RFSwitch(config-if)#storm-control ucast ratelimit 88
RFSwitch(config-if)#
```

13

Spanning tree-mst Instance

Use the `(config-mst)` instance to configure the switch's *Multi Spanning Tree Protocol* (MSTP) configuration. To switch to this instance, use the command:

```
RFSwitch(config)#spanning-tree mst configuration
RFSwitch(config-mst)#
```

13.1 mst Config Commands

Table 13.1 summarizes the **`(config-mst)`** commands:

Table 13.1 MSTI configuration commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 13-3*
end	Ends the current mode and moves to the EXEC mode	*page 13-4*
exit	Ends the current mode and moves to the previous mode	*page 13-5*
help	Displays the system's interactive help system	*page 13-6*
instance	Assigns a VLAN to the bridge instance	*page 13-7*
name	Sets a name for the MST region	*page 13-8*
no	Negates a command or sets defaults	*page 13-9*
revision	Configures the revision number of the MST bridge	*page 13-10*

Command	***Description***	***Ref.***
service	Invokes service commands needed to troubleshoot or debug `(config-if)` instance configurations	*page 13-11*
show	Shows running system information	*page 13-13*

13.1.1 clrscr

mst Config Commands

Clears the display

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-mst)#clrscr
RFSwitch(config-mst)#
```

13.1.2 end

mst Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-mst)#end
RFSwitch#
```

13.1.3 exit

mst Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-mst)#exit
RFSwitch(config)#
```

13.1.4 help

mst Config Commands

Displays the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-mst)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-mst)#
```

13.1.5 instance

mst Config Commands

Associates VLAN(s) with an instance

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
instance <1-15> vlan <vlan-id>
```

Parameters

<1-15>	Defines the instance ID to which the VLAN is associated
vlan <vlan-id>	Sets the VLAN ID for its association with an instance

Usage Guidelines

MSTP works based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Switches with the same instance, VLAN mapping, revision number and region names define a unique region. Switches in the same region exchange *bridge protocol data units* (BPDUs) with instance record information within it.

Example

The following example sets an instance named 10 and maps VLAN 20 to it:

```
RFSwitch(config-mst)#instance 10 vlan 20
RFSwitch(config-mst)#
```

13.1.6 name

mst Config Commands

Sets the name for the MST region

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
name <region-name>
```

Parameters

<region-name>	Sets MST region name

Example

```
RFSwitch(config-mst)#name MyRegion
RFSwitch(config-mst)#
```

13.1.7 no

mst Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [instance|name|revision]
```

Parameters

instance	Sets the MST Instance • vlan – Delete the association of vlan with this instance • <vlan-id> – List of vlan IDs
name	Assigns a name to the MST region
revision	Defines the revision number for configuration information

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFSwitch(config-mst)#no instance 10 vlan 20
RFSwitch(config-mst)#

RFSwitch(config-mst)#no name MyRegion
RFSwitch(config-mst)#

RFSwitch(config-mst)#no revision
RFSwitch(config-mst)#
```

13.1.8 revision

mst Config Commands

Sets the revision number of the MST bridge

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
revision <0-255>
```

Parameters

revision <0-255>	Defines the revision number for configuration information

Example

```
RFSwitch(config-mst)#revision 20
RFSwitch(config-mst)#
```

13.1.9 service

mst Config Commands

Invokes service commands needed to troubleshoot or debug (`config-if`) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-mst)#service show cli
MSTI configuration mode:
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-instance
  +-<1-15> [instance <1-15>]
    +-vlan
      +-VLAN_ID [instance <1-15> vlan VLAN_ID]
+-name
  +-LINE [name LINE]
+-no
  +-instance
    +-<1-15> [no instance <1-15>]
      +-vlan
        +-VLAN_ID [no instance <1-15> vlan VLAN_ID]
  +-name [no name]
  +-revision [no revision]
+-quit [quit]
+-revision
  +-REVISION_NUM [revision REVISION_NUM]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
```

```
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
    +-cli [service show cli]
+-show
  +-access-list [show access-list]
    +-<1-99> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-<100-199> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-<1300-1999> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-<2000-2699> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-WORD [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
  +-aclstats
    +-vlan
      +-<1-4094> [show aclstats ( vlan <1-4094>
)].................
...........................................................
.......
...........................................................
.......

RFSwitch(config-mst)#
```

13.1.10 show

mst Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-mst)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy             Display redundancy group parameters
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  snmp                   Display SNMP engine parameters
  smtp-notification      Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged                          in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-mst)#show
```

14

Extended ACL Instance

The Extended ACL instance `(config-ext-nacl)` is used to manage the extended Access Control List entries associated with the switch.

To navigate to this instance, use the command

```
RFSwitch(config)#ip access-list extended [<ACL-name>|
  <100-199>|<2000-2699>]
RFSwitch(config-ext-nacl)#
```

14.1 Extended ACL Config Commands

Table 14.1 summarizes **`config-ext-nacl`** commands:

Table 14.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 14-3*
deny	Specifies packets to reject	*page 14-4*
exit	Ends the current mode and moves to the previous mode	*page 14-11*
help	Displays the interactive help system	*page 14-12*
mark	Specifies packets to mark	*page 14-13*
no	Negates a command or sets its defaults	*page 14-19*

Table 14.1 Extended ACL Config Command Summary (Continued)

Command	Description	Ref.
permit	Specifies packets to forward	*page 14-20*
service	Invokes the service commands to troubleshoot or debug `(config-if)` instance configurations	*page 14-25*
show	Displays running system information	*page 14-26*

14.1.1 clrscr

Extended ACL Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-ext-nacl)#clrscr
RFSwitch(config-ext-nacl)#
```

14.1.2 deny

Extended ACL Config Commands

Specifies packets to reject

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

deny [icmp|ip|tcp|upd]

deny icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}*

deny ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*

deny [tcp|udp] [<source-IP/Mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*

Parameters

deny ip [<source-IP/ Mask>|any|host <IP>][<dest-IP/ Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **deny** command to reject IP packets • deny – Sets the action type on an ACL • ip – Specifies an IP (to match to a protocol) • <source-ip/mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <ip> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

deny icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}*	Use with the **deny** command to reject ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-ip/mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

deny [tcp|udp] [<source-IP/Mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>]*{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*	Use with the **deny** command to reject TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/Mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocol types are supported:

- ip
- icmp
- tcp
- udp

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select the ICMP as the protocol to allow/deny ICMP packets. Selecting icmp provides the option of filtering icmp packets based on icmp type and code



NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

14.1.2.1 Example - Denying Traffic Between Two Subnets

The following example denies traffic between two subnets:

```
     RFSwitch(config-ext-nacl)#deny ip 192.168.2.0/24
192.168.1.0/24
     RFSwitch(config-ext-nacl)#permit ip any any
     RFSwitch(config-ext-nacl)#
```

14.1.2.2 Example - Denying TCP Based Traffic

The following example denies TCP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
      RFSwitch(config-ext-nacl)#deny tcp range 20 23
192.168.1.0/24 192.168.2.0/24

     RFSwitch(config-ext-nacl)#permit ip any any
     RFSwitch(config-ext-nacl)#
```

14.1.2.3 Example - Denying UDP Based Traffic

The following example denies UDP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
      RFSwitch(config-ext-nacl)#deny udp range 20 23
192.168.1.0/24 192.168.2.0/24

     RFSwitch(config-ext-nacl)#permit ip any any
     RFSwitch(config-ext-nacl)#
```

14.1.2.4 Example - Denying ICMP Based Traffic

The following example denies ICMP traffic from any source to any destination. The keyword *any* is used to match:

```
     any source or destination IP address.
     RFSwitch(config-ext-nacl)#deny icmp any any
     RFSwitch(config-ext-nacl)#permit ip any any
     RFSwitch(config-ext-naclend
```

14.1.3 end

Extended ACL Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-ext-nacl)#end
RFSwitch#
```

14.1.4 exit

Extended ACL Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-ext-nacl)#exit
RFSwitch(config)#
```

14.1.5 help

Extended ACL Config Commands

Displays the system's interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-ext-nacl)#
```

14.1.6 mark

Extended ACL Config Commands

Specifies packets to mark

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

mark [8021p|dscp|tos]

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>] [icmp|ip|tcp|udp]

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>] icmp [<source-ip/mask>|any|host <ip>] [<dest-ip/mask>|any|host <ip>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>] ip [<source-ip/mask>|any|host <ip>] [<dest-ip/mask>|any|host <ip>] *{log} {rule-precedence <1-5000>}*

mark [8021p <vlan-priority-value>|dscp <dscp-codepoint-value>|tos <tos-value>] [tcp|udp] [<source-ip/mask>|any|host <ip>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-ip/mask|any|host <ip>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*

Parameters

8021p <vlan-priority-value>	Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7).
dscp <dscp-codepoint-value>	Sets the Differentiated Services Code Point code-point value to <dscp-codepoint-value> (0-63)
tos <tos-value>	Sets the TOS value to <tos-value>. The least significant two bits of the <tos-value> must be 0.

ip [<source-IP/ Mask>|any|host <IP>] [<dest-IP/Mask>| any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with **mark** command to mark a packet. • ip – Specifies an IP (to match to a protocol) • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

icmp [<source-IP/ mask>|any|host <IP>] [<dest-IP/Mask>|any| host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*	Use with the **mark** command to mark ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-IP/mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

[tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq <source-port>|range <starting-source-port> <ending-source-port>} [<dest-IP/Mask|any|host <IP>] {eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}	Use with the **mark** command to mark TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/Mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Marks traffic between networks/hosts based on the protocol type selected in the access list configuration

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

The following types of protocols are supported:

- ip
- icmp
- tcp
- udp

Whenever the interface receives the packet, its content is checked against all ACEs in the ACL. It is marked based on the ACL configuration

- Filtering protocol types TCP/UDP allow the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny ICMP packets (selecting ICMP allows you to filter packets based on the ICMP type and code)



NOTE: The log option is functional only for router ACL's. The log option provides an informational logging message about the packet matching the entry sent to the console.

14.1.6.1 Example - Marking dot1p on TCP Based Traffic

The example below marks the dot1p priority value in the ethernet header to 5 on all TCP traffic coming from the source subnet:

```
RFSwitch(config-ext-nacl)# mark 8021p 6 udp 192.168.2.0/24
range 5060 5061
RFSwitch(config-ext-nacl)#
```

14.1.6.2 Example - Marking tos on TCP based Traffic

The example below marks the tos value in the IP header to 245 on all tcp traffic coming from the source subnet:

```
RFSwitch(config-ext-nacl)# mark tos 160 udp 192.168.2.0/24
range 5060 5061
RFSwitch(config-ext-nacl)#

RFSwitch(config-ext-nacl)# mark dscp 40 udp 192.168.2.0/24
range 5060 5061
RFSwitch(config-ext-nacl)#
```

14.1.7 no

Extended ACL Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [deny|mark|permit]
```

Negates all the syntax combinations used in the deny, mark and permit designations to configure the Extended ACL

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command.

Example

```
RFSwitch(config-ext-nacl)#no mark 8021p 5 tcp 192.168.2.0/24
any rule-precedence 10
RFSwitch(config-ext-nacl)#

RFSwitch(config-ext-nacl)#no permit ip any any rule-
precedence 10
RFSwitch(config-ext-nacl)#

RFSwitch(config-ext-nacl)#no deny icmp any any rule-
precedence 10
RFSwitch(config-ext-nacl)#
```

14.1.8 permit

Extended ACL Config Commands

Permits specific packets.



NOTE: ACLs do not allow DHCP messages to flow by default. Configure an *Access Control Entry* (ACE) to allow DHCP messages to flow through.

```
RFSwitch(config-ext-nacl)#permit ip xxx.xxx.xxx.xxx/
x 192.168.2.0/24

RFSwitch(config-ext-nacl)#permit ip any host
xxx.xxx.xxx.xxx

RFSwitch(config-ext-nacl)#
```

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

permit[icmp|ip|tcp|upd]

permit icmp [<source-IP/Mask>|any|host <ip>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*

permit ip [<source-IP/Mask>|any|host <IP>] [<dest-IP/mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*

permit [tcp|udp] [<source-ip/mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*

Parameters

permit ip [<source-IP/ Mask>|any|host <IP>] [<dest-IP/mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **`permit`** command to allow IP packets • deny – Sets the action type on an ACL • IP – Specifies an IP (to match to a protocol) • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address. • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

permit icmp [<source-IP/Mask>|any|host <ip>] [<dest-IP/Mask>|any|host <IP>] *{<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]}*	Use with the **`permit`** command to allow ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • [<source-IP/Mask>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format). The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • [<dest-IP/Mask>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

permit [tcp|udp] [<source-ip/mask>|any|host <IP>] *{eq <source-port>|range <starting-source-port> <ending-source-port>}* [<dest-IP/Mask|any|host <IP>] *{eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}*	Use with the **`permit`** command to allow TCP or UDP packets • deny – Rejects TCP or UDP packets • tcp|udp – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535. • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/mask|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port>} {range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- ip

- icmp
- tcp
- udp

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets. Selecting ICMP allows to filter ICMP packets based on type and code



NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

14.1.8.1 Permitting IP Based Traffic

The example below allows IP traffic from the source subnet to the destination subnet and denies all other traffic over an interface:

```
RFSwitch(config-ext-nacl)#permit ip 192.168.1.10/24
192.168.2.0/24 rule-precedence 40
RFSwitch(config-ext-nacl)#
```

14.1.8.2 Permitting Telnet Based Traffic

The example below permits Telnet traffic from the source subnet and the destination subnet and denies all other traffic over an interface:

```
RFSwitch(config-ext-nacl)#permit tcp 192.168.4.0/24
192.168.5.0/24 eq 23 rule-precedence 10
RFSwitch(config-ext-nacl)#
```

14.1.8.3 Permitting ICMP Based Traffic

The example below permits ICMP traffic and denies all other traffic over an interface:

```
RFSwitch(config-ext-nacl)#permit icmp any any rule-
precedence 30
RFSwitch(config-ext-nacl)#)#
```

14.1.9 service

Extended ACL Config Commands

Invokes service commands to troubleshoot or debug the `(config-if) instance` configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-ext-nacl)#service show cli
Extended ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-icmp
    +-A.B.C.D/M
      +-A.B.C.D/M [(deny|permit|mark (8021p <0-7> | tos <0-
255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M |
host A.B.C.D | any)(<0-255> | <0-255> <0-255> |)(log|)(rule-
precedence <1-5000> |)]
        +-<0-255> [(deny|permit|mark (8021p <0-7> | tos <0-
255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M |
host A.B.C.D | any)(<0-255> | <0-255> <0-255> |)(log|)(rule-
precedence <1-5000> |)]
          +-<0-255> [(deny|permit|mark (8021p <0-7> | tos
<0-255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M
| host A.B.C.D | any)(<0-255> | <0-255> <0-255>
|)(log|)(rule-precedence <1-5000> |)]
            +-log [(deny|permit|mark (8021p <0-7> | tos <0-
255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M |
host A.B.C.D | any)(<0-255> | <0-255> <0-255> |)(log|)(rule-
precedence <1-5000> |)]
+-rule-precedence
.....................................................
.....................................................
.....................................................
RFSwitch(config-ext-nacl)#
```

14.1.10 show

Extended ACL Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-ext-nacl)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  environment            show environmental information
  file                   Display filesystem information
  firewall              Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy     Display redundancy group parameters
  role                  Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notifications    Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged                          in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFS6000(config-ext-nacl)#show
```

14.2 Configuring IP Extended ACL

IP Extended ACLs contain rules based on the following parameters:

- Source IP address
- Destination IP address
- IP Protocol
- Source Port–if protocol is TCP or UDP
- Destination Port–if protocol is TCP or UDP
- ICMP Type–if protocol is ICMP
- ICMP Code–if protocol is ICMP

IP protocol, Source IP and Destination IP are mandatory parameters.You can create either a *Numbered IP Extended ACL* or a *Named IP Extended IP Address*.

Execute the following commands to configure an IP Extended ACL:

1. To configure a numbered IP Extended ACL:

```
RFSwitch(config)#access-list 2 deny ip host 1.2.3.4 any rule-
precedence 10
RFSwitch(config)#access-list 2 permit tcp any host 2.3.4.5 eq 80
rule-precedence 20
RFSwitch(config)#access-list 2 deny icmp any host 2.3.4.5 rule-
precedence 30
```

2. To configure named IP Extended ACL:

```
RFSwitch(config)#ip access-list extended ipextacl
RFSwitch(config-ext-nacl)#deny ip host 1.2.3.4 any rule-
precedence 10
RFSwitch(config-ext-nacl)#permit tcp any host 2.3.4.5 eq 80
rule-precedence 20
RFSwitch(config-ext-nacl)#deny icmp any host 2.3.4.5 rule-
precedence 30
```

15

Standard ACL Instance

The Standard ACL instance (`config-std-acl`) is used to manage the standard Access Control List entries associated with the switch.

To navigate to this instance, use the command:

```
RFSwitch(config)#ip access-list standard [<ACL-name>|
  <1-99>|<1300-1999>]
RFSwitch(config-std-acl)#
```

15.1 Standard ACL Config Commands

Table 15.1 summarizes the **`config-std-nacl`** commands:

Table 15.1 Standard ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 15-3*
deny	Specifies packets to reject	*page 15-4*
end	Ends the current mode and moves to the EXEC mode	*page 15-6*
exit	Ends the current mode and moves to the previous mode	*page 15-7*
help	Displays the interactive help system	*page 15-8*
mark	Specifies packets to mark	*page 15-9*
no	Negates a command or sets its defaults	*page 15-11*

Table 15.1 Standard ACL Config Command Summary (Continued)

Command	Description	Ref.
permit	Specifies packets to forward	*page 15-12*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 15-14*
show	Displays running system information	*page 15-16*

15.1.1 clrscr

Standard ACL Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-std-nacl)#clrscr
RFSwitch(config-std-nacl)#
```

15.1.2 deny

Standard ACL Config Commands

Specifies packets to reject

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`deny [<source-IP/Mask>|any|host <IP>] {log} {rule-precedence <1-5000>}`

Parameters

[<source-IP/ Mask>|any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a deny command to reject packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL..

Usage Guidelines

Use this command to deny traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.



NOTE: The log option is functional only for router ACL's. The log option results in an informational logging message for the packet matching the entry sent to the console.

15.1.2.1 Example - Denying Traffic to the Interface

The example below denies all traffic entering the interface (a log message is generated whenever the interface receives a packet):

```
RFSwitch(config-std-nacl)#deny any log rule-precedence 50
RFSwitch(config-std-nacl)#
```

15.1.2.2 Example - Denying Traffic only from Source Network

The example below denies traffic from the source network (xxx.xxx.1.0/24) and allows all other traffic to flow through the interface:

```
RFSwitch(config-std-nacl)#deny xxx.xxx.1.0/24 rule-
precedence 60
RFSwitch(config-std-nacl)#permit any
```

15.1.3 end

Standard ACL Config Commands

Ends and exits from the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-std-nacl)#end
RFSwitch#
```

15.1.4 exit

Standard ACL Config Commands

Ends the current mode and moves to previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-std-nacl)#exit
RFSwitch(config)#
```

15.1.5 help

Standard ACL Config Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-std-nacl)#
```

15.1.6 mark

Standard ACL Config Commands

Specifies packets to mark

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mark [8021p|dscp|tos]
mark 8021p <vlan-priority-value>
mark dscp <dscp-codepoint-value>
mark tos <tos-value> [<source-IP/Mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}
```

Parameters

8021p <vlan-priority-value>	Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7).
dscp <dscp-codepoint-value>	Sets the Differentiated Services Code Point code-point value to <dscp-codepoint-value> (0-63)
tos <tos-value>	Sets the TOS value to <tos-value>. The least significant two bits of the <tos-value> must be 0.

[<source-IP/Mask>| any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **`mark`** command to mark packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Optional.Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to mark traffic from the source network/host. Use the mark option to specify the t*ype of service* (TOS) and priority value. The TOS value is marked in the IP header. The 802.1p priority value is marked in the frame.

When the interface receives the packet, its content is checked against the ACEs in the ACL. It is marked based on the ACL configuration.



NOTE: The log option is functional only for router ACLs. The log option results in an informational logging message about the packet matching the entry sent to the console.

15.1.6.1 Marking tos for Source Network Traffic

The example below marks the *type of service* (TOS) value to 254 for all traffic coming from the source network:

```
RFSwitch(config)#access-list 3 mark tos 254 xxx.xxx.3.0/24
RFSwitch (config)#access-list 3 permit any
```

15.1.7 no

Standard ACL Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [deny|mark|permit]
```

Negates all the syntax combinations used in deny, mark and permit designations.

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
RFSwitch(config-std-nacl)#no permit any rule-precedence 10
RFSwitch(config-std-nacl)#

RFSwitch(config-std-nacl)#no deny any rule-precedence 20
RFSwitch(config-std-nacl)#

RFSwitch(config-std-nacl)#no mark tos 4 192.168.2.0/24 rule-
precedence 30
RFSwitch(config-std-nacl)#
```

15.1.8 permit

Standard ACL Config Commands

Specifies packet to forward

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
permit [<source-IP/Mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}
```

Parameters

[<source-IP/Mask>| any|host <IP>] *{log} {rule-precedence <1-5000>}*	Use with a **permit** command to allow packets • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. The <Mask> is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to allow traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL's configuration.



NOTE: The log option is functional only for router ACLs. The log option displays an informational logging message about the packet matching the entry sent to the console.

15.1.8.1 Example - Permitting Traffic to Interface

The example below permits all the traffic that comes to the interface:

```
RFSwitch(config-std-nacl)#permit any rule-precedence 50
RFSwitch(config-std-nacl)#
```

15.1.8.2 Permitting Traffic from Source Network

The example below permits traffic from the source network and provides a log message:

```
RFSwitch(config-std-nacl)#permit xxx.xxx.1.0/24 log rule-
precedence 60
RFSwitch(config-std-nacl)#
```

15.1.9 service

Standard ACL Config Commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

cli	Displays the CLI tree of the current mode

Example

```
RFSwitch(config-std-nacl)#service show cli
Standard ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-A.B.C.D/M [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
    +-log [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
      +-rule-precedence
        +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
    +-rule-precedence
      +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
  +-any [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
    +-log [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
      +-rule-precedence
```

```
        +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
    +-rule-precedence
      +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence
<1-5000> |)]
.............................................................
.............................................................
.............................................................
.....................
RFSwitch(config-std-nacl)#
```

15.1.10 show

Standard ACL Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command

Example

```
RFSwitch(config-std-nacl)#show ?
access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
 environment            show environmental information
  file                   Display filesystem information
  firewall              Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy     Display redundancy group parameters
  rtls                   Real Time Locating System commands
  role                  Configure role parameters
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notifications    Display the SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged  in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-std-nacl)#show
```

15.2 Use Case: Configuring IP Standard ACL

IP Standard ACLs contain rules based on *Source IP Address*. You can create either a *Numbered IP Standard ACL* or a *Named IP Standard IP Address*.

Execute the following CLI commands to configure an IP based standard ACL:

1. To configure numbered IP Standard ACL:

   ```
   RFSwitch(config)#access-list 2 deny host 1.2.3.4 rule-precedence
   10
   RFSwitch(config)#access-list 3 deny host 1.2.3.4 rule-precedence
   10
   RFSwitch(config)#access-list 3 permit any rule-precedence 20
   ```

   Valid numbers for numbered IP Standard ACLs are from 1-99 and 1300-1999. In the above CLI example, ACL 3 denies host with IP 1.2.3.4 and allows all other hosts.

2. To configure an IP Standard ACL:

   ```
   RFSwitch(config)#ip access-list standard ipst2
   RFSwitch(config-std-nacl)#permit host 10.1.1.10 rule-precedence
   30
   RFSwitch(config-std-nacl)#deny any rule-precedence 20
   ```

16

Extended MAC ACL Instance

Use the `(config-ext-macl)` instance to configure `mac access-list extended` ACLs. To navigate to this instance, use the command:

```
RFSwitch(config)#mac access-list extended <acl-name>
RFSwitch(config-ext-macl)#
```

16.1 MAC Extended ACL Config Commands

Table summarizes **`config-ext-macl`** commands:

Table 16.1 MAC Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 16-3*
deny	Specifies packets to reject	*page 16-4*
end	Ends the current mode and moves to the EXEC mode	*page 16-8*
exit	Ends the current mode and moves to the previous mode	*page 16-9*
help	Displays the interactive help system	*page 16-10*
mark	Specifies packets to mark	*page 16-11*
no	Negates a command or sets its defaults	*page 16-14*
permit	Specifies packets to forward	*page 16-15*

Table 16.1 MAC Extended ACL Config Command Summary (Continued)

Command	Description	Ref.
service	Invokes service commands to troubleshoot or debug the `(config-if)` instance configurations	*page 16-19*
show	Shows running system information	*page 16-21*

16.1.1 clrscr

MAC Extended ACL Config Commands

Clears the display screens

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-ext-macl)#clrscr
RFSwitch(config-ext-macl)#
```

16.1.2 deny

MAC Extended ACL Config Commands

Specifies packets to reject



NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny/mark` designation for a packet. The command set for Extended MAC ACLs provide the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
  host <MAC>] {[dot1p|rule-precedence|type|vlan]}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
  host <MAC>] dot1p <0-7> {rule-precedence|type}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
  host <MAC>] rule-precedence <1-5000>

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
  host <MAC>] type [8021p|<1-65535>|aarp|appletalk|apr|ip|
ipv6|ipx|rarp|wisp] {rule-precedence <precedence>}

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any|
  host <MAC>] vlan <1-4094> {rule-precedence|type}
```

Parameters

deny [<MAC/Mask>|any|host <MAC>] [<MAC/Mask>|any| host <MAC>] {[dot1p| rule-precedence|type|vlan]}	Define a source and destination MAC address and Mask specifying the bits to match. The source and destination wildcards can be any one of the following: • [<MAC/Mask>|any|host <MAC>]– Source MAC address and mask in the format **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx.** • any – Any source host • host **–** Exact source MAC address to match
dot1p <0-7>	Determine a 802.1p priority value to match. <priority> is in the range 0 to 7.
rule-precedence <1-5000>	Define an access-list entry precedence
type [8021q|<1-65535>| arp|appletalk|ip|ipv6|vlan|ipx|arp| wisp]	Set an ethertype value represented as an integer. Use keywords for well-known ethertypes (IP, IPv6, ARP etc.) • 8021q **– VLAN Ether type (0*8100)** • <1-65535> **– Ether protocol number** • aarp **– AARP Ether Type (0*80F3)** • appletalk **– APPLETALK Ether Type (0*809B)** • arp **– ARP Ether Type (0*0806)** • ip **– IP Ether Type (0*0800)** • ipv6 **– IPv6 Ether Type (0*86DD)** • ipx **– IPX Ether Type (0*8137)** • rarp **– RARP Ether Type (0*8035)** • wisp **– WISP Ether Type (0*8783)**

vlan<1-4095>	Set a VLAN tag ID to match

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and ethertype.

The most common ethertypes are:

- arp
- wisp
- ip
- 802.1q



NOTE: MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

16.1.2.1 Example - Denying Traffic from any MAC Address

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
RFSwitch(config-ext-macl)#deny any host 00:01:ae:00:22:11
RFSwitch(config-ext-macl)#
```

16.1.2.2 Example - Denying dot1q Tagged Traffic

The MAC ACL (in the example below) denies dot1q tagged traffic from VLAN interface 5:

```
RFSwitch(config-ext-macl)#deny any any vlan 5 type 8021q
RFSwitch(config-ext-macl)#
```

16.1.2.3 Example - Denying Traffic Between Two MAC Based Hosts

The example below denies traffic between two hosts based on MAC addresses:

```
RFSwitch(config-ext-macl)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
RFSwitch(config-ext-macl)#
```

16.1.3 end

MAC Extended ACL Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-ext-macl)#end
RFSwitch#
```

16.1.4 exit

MAC Extended ACL Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-ext-macl)#exit
RFSwitch(config)#
```

16.1.5 help

MAC Extended ACL Config Commands

Displays the system's interactive help (in HTML format)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-ext-macl)#
```

16.1.6 mark

MAC Extended ACL Config Commands

Specifies the packet to mark



NOTE: Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equivalent of the ethertype listed in the CLI or any other type of ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mark [8021p|dscp|tos]
mark [8021p <vlan-priority-value>|dscp
<dscp-codepoint-value>|tos <tos-value>] [icmp|ip|tcp|udp]
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] icmp [<source-IP/
Mask>|any|host<IP>] [<dest-IP/mask>|any|host <IP>]
{<ICMP-type> {<ICMPcode>}}
{log} {rule-precedence <1-5000>]}
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] IP [<source-IP/
mask>|any|host <IP>][<dest-ip/mask>|any|host <IP>] {log}
{rule-precedence <1-5000>}
mark [8021p <vlan-priority-value>|dscp
<dscp-codepointvalue>|tos <tos-value>] [tcp|udp]
[source-IP/Mask>|any|host<IP>] {eq <source-port>|range
<starting-source-port> <ending-source-port>} [<dest-IP/
Mask|any|host <IP>] {eq <source-port>} {range
<starting-source-port> <ending-sourceport>}{log}
{rule-precedence <1-5000>}
```

Parameters

8021p<*0-7*>	Modifies the 802.1p VLAN user priority • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
tos<*0-255*>	Modifies the TOS bits in an IP header • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Destination MAC address and mask • any – Any destination host • host **–** Exact destination MAC address to match
mark [<source-IP/Mask> |any|host<IP>]	Specifies the bits to match. The source wildcard can be any one of the following: • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
mark [<dest-IP/mask>|any|host <IP>]	Specifies bits to match. The destination wildcard can be any one of the following: • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match
dot1p<*0-7*>	Defines a VLAN 802.1p priority value to match
rule-precedence<*1-5000*>	Establishes an access-list entry precedence

type [8021q|*<1-65535>*| arp|appletalk|ip|ipv6ipx|rarp| vlan|wisp]	Defines an ethertype value represented as an integer or keyword for well-known ethertypes (like IP, IPv6, ARP etc.)
vlan *<1-4095>*	Defines the VLAN tag ID to match
dscp <0-63>	Modify DSCP TOS bits in IP header • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match

Usage Guidelines

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.

16.1.6.1 Example - Marking dot1p Priority Value for 802.1q Tagged Traffic

The example below marks the dot1p priority value to 6 for all 802.1q tagged traffic from VLAN interface 5:

```
RFSwitch(config-ext-macl)#mark 8021p 6 any any vlan 5 type
8021q
RFSwitch(config-ext-macl)#
```

16.1.6.2 Example - Marking tos for IP Traffic

The example below marks the tos field to 254 for IP traffic coming from the source MAC :

```
RFSwitch(config-ext-macl)#mark tos 254 host
00:33:44:55:66:77 any type ip
RFSwitch(config-ext-macl)#
```

16.1.7 no

MAC Extended ACL Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [deny|mark|permit]
```

Negates all the syntax combinations used in deny, mark and permit designations to configure the Extended ACL

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
RFSwitch(config-ext-macl)#no mark tos 254 host
00:33:44:55:66:77 any type ip rule-precedence 50
RFSwitch(config-ext-macl)#

RFSwitch(config-ext-macl)#no deny any any vlan 5 type 8021q
rule-precedence 10
RFSwitch(config-ext-macl)#

RFSwitch(config-ext-macl)#no permit any any type wisp rule-
precedence 50
RFSwitch(config-ext-macl)#
```

16.1.8 permit

MAC Extended ACL Config Commands

Specifies packets to forward



NOTE: Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equivalent of the ethertype listed in the CLI or any other type of ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
permit [icmp|ip|tcp|upd]
permit icmp [<source-IP/Mask>|any|host <IP>] [<dest-IP/
Mask>|any|host <IP>] {<ICMP-type> {<ICMP-code>}} {log}
{rule-precedence <1-5000>]}

permit ip [<source-IP/mask>|any|host <ip>] [<dest-IP/
Mask>|any|host <ip>] {log} {rule-precedence <1-5000>}

permit [tcp|udp] [<source-IP/Mask>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-sourceport>}[<dest-IP/Mask|any|host <IP>] {eq
<source-port>}{range <starting-source-port>
<ending-source-port>} {log}{rule-precedence <1-5000>}
```

Parameters

permit [<source-IP/ Mask>|any|host <IP>]	Specifies the bits to match. The source wildcard can be any one of the following: • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Source MAC address and mask • any – Uses any source host • host – Defines the MAC address to match

permit [<dest-IP/ Mask>|any|host <IP>] {<ICMP-type> {<ICMP-code>}}	Bit mask specifying the bits to match. The destination wildcard can be one of the following: • **xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx**–Destination MAC address and mask • any – Uses any available destination host • host – Defines the destination MAC address
dot1p*<0-7>*	Establishes the 802.1p priority
rule-precedence*<1-5000>*	Defines an access list entry precedence
type(8021q|*<1-65535>*|aarp|arp|appletalk|ip|ipv6|ipx|rarp|vlan|wisp)	Sets an ethertype • 8021q **–VLAN Ether type (0*8100)** • <1-65535> **– Ether protocol number** • aarp **– AARP Ether Type (0*80F3)** • appletalk **– APPLETALK Ether Type (0*809B)** • arp **– ARP Ether Type (0*0806)** • ip **– IP Ether Type (0*0800)** • ipv6 **– IPv6 Ether Type (0*86DD)** • ipx **– IPX Ether Type (0*8137)** • rarp **– RARP Ether Type (0*8035)** • wisp **– WISP Ether Type (0*8783)**
vlan*<1-4095>*	Sets the VLAN ID

Usage Guidelines

When creating a Port ACL, the switch (by default) does not permit an ethertype WISP. Create a rule to allow WISP to adopt access ports. Use the following command to adopt access ports:

```
permit any any type wisp
```

NOTE: Use the following command to attach a MAC access list to a port on a layer 2 interface:

```
mac access-group <acl number/name> in
```

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, ethernet type. Common types include:

- arp
- wisp
- ip
- 802.1q

The switch (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access port through an interface, configure an access control list to allow an ethernet WISP. .

NOTE: To apply an IP based ACL to an interface, a MAC access list entry to allow ARP is mandatory. A MAC ACL always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/ denied based on the ACL's configuration.

16.1.8.1 Example - Permitting WISP Traffic

The example below permits WISP traffic from any source MAC address to any destination MAC address:

```
RFSwitch(config-ext-macl)#permit any any type wisp
RFSwitch(config-ext-macl)#
```

16.1.8.2 Example - Permitting ARP Traffic

The example below permits arp based traffic from any source MAC address to any destination MAC address:

```
RFSwitch(config-ext-macl)#permit any any type arp
RFSwitch(config-ext-macl)#
```

16.1.8.3 Permitting IP Traffic

The example below permits IP based traffic from a source MAC address to any destination MAC address:

```
RFSwitch(config-ext-macl)#permit host 11:22:33:44:55:66 any
type ip
RFSwitch(config-ext-macl)#
```

16.1.9 service

MAC Extended ACL Config Commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

show cli	Displays running system information

Example

```
RFSwitch(config-ext-macl)#service show cli
MAC Extended ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX
    +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX [(deny|permit|mark
(8021p <0-7> | tos
<0-255>))(XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host
XX:XX:XX:XX:XX:XX | any)(XX
:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(vlan <1-4095>
| dot1p <0-7> |) (type (<1-65535> | ip | ipv6          | arp
| wisp | 8021q | ra
rp | aarp | appletalk | ipx ) |)(rule-precedence <1-5000>
|)]
      +-dot1p
        +-<0-7> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(XX:XX:XX:XX:XX:X
X/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:XX:XX:X
X:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095> |
dot1p <0-7> |) (type (<1
-65535> | ip | ipv6          | arp | wisp | 8021q | rarp |
aarp | appletalk | ip
x ) |)(rule-precedence <1-5000> |)]
```

```
          +-rule-precedence
            +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos
<0-255>))(XX:XX:XX:
XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:
XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095>
| dot1p <0-7> |) (t
ype (<1-65535> | ip | ipv6          | arp | wisp | 8021q |
rarp | aarp | appleta
lk | ipx ) |)(rule-precedence <1-5000> |)]
          +-type
.............................................................
.............................................................
.............................................................
.....................
RFSwitch(config-ext-macl)#
```

16.1.10 show

MAC Extended ACL Config Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power
- The following commands display only for RFS7000 port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Usage Guidelines

The `show access-list` command displays the access lists configured for the switch. Provide the access list name or number to view specific ACL details

Example

```
RFSwitch(config-ext-macl)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
```

```
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  dpd                  wios dataplane
  environment           show environmental information
  file                  Display filesystem information
  firewall             Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name             Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy           Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                 Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
  smtp-notofication    Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration
parameters
  traffic-shape        Display traffic shaping
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
```

```
  users                  Display information about currently
logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

RFSwitch(config-ext-macl)#show
```

16.2 Configuring MAC Extended ACL

MAC Extended ACLs contain rules based on the following parameters:

- Source MAC address
- Destination MAC address
- Ethertype– accepts well known types like IP, ARP, VLAN or an integer value between 1-65535.
- VLAN-ID
- VLAN 802.1p user priority

Source and Destination MAC address are mandatory parameters.

Execute the following commands to configure a MAC extended ACL with different rule parameters on the switch:

```
RFSwitch(config)#mac access-list extended macextacl
RFSwitch(config-ext-macl)#permit 00:a0:f8:00:00:00
ff:ff:ff:00:00:00 any rule-precedence 10
RFSwitch(config-ext-macl)#deny any any type arp rule-precedence
20
RFSwitch(config-ext-macl)#deny any any vlan 23 rule-precedence
30
```

17

DHCP Server Instance

Use the `(config-dhcp)` instance to configure the DHCP server address pool associated with the switch.

To move to this instance, use the command.

```
RFSwitch(config)#ip dhcp pool <pool-name>
RFSwitch(config-dhcp)#
```

Also refer to Chapter12, section 12.1.8 ip on page 12-20 for other DHCP related configurations.

17.1 DHCP Config Commands

Table 17.1 summarizes **`config-dhcp`** commands:

Table 17.1 DHCP Server Command Summary

Command	Description	Ref.
address	Defines the DHCP server include range	*page 17-4*
bootfile	Assigns a boot file name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted	*page 17-5*
class	Associates a class with a pool and moves to the DHCP pool class configuration mode	*page 17-6*
client-identifier	Uses an ASCII string as a client identifier	*page 17-9*

Table 17.1 DHCP Server Command Summary

Command	Description	Ref.
client-name	Assigns a client name	*page 17-10*
clrscr	Clears the display screen	*page 17-11*
ddns	Configures *Dynamic DNS* (DDNS) values	*page 17-12*
default-router	Configures a default router's IP address	*page 17-14*
dns-server	Sets the IP address of a DNS Server	*page 17-15*
domain-name	Sets the domain name	*page 17-16*
end	Ends the current mode and moves to the EXEC mode	*page 17-17*
exit	Ends the current mode and moves to the previous mode	*page 17-18*
hardware-address	Defines the hardware address using either a dashed or dotted hexadecimal string	*page 17-19*
help	Displays the interactive help system in HTML format	*page 17-20*
host	Configures an IP address for the host	*page 17-21*
lease	Assigns the lease time for a DHCP leased IP address	*page 17-22*
netbios-name-server	Configures NetBIOS (WINS) name servers	*page 17-24*
netbios-node-type	Defines the NetBIOS node type	*page 17-25*
network	Sets a network number and mask for a DHCP Server	*page 17-26*
next-server	Configures the next server in boot process	*page 17-27*
no	Negates a command or sets its defaults	*page 17-28*
option	Assigns a name for a DHCP option	*page 17-29*

Table 17.1 DHCP Server Command Summary

Command	Description	Ref.
service	Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations	*page 17-30*
show	Displays the running system information	*page 17-31*
unitcast-enable	Enables unicast for DHCP	*page 17-34*
update	Controls the usage of *Dynamic DNS* (DDNS)	*page 17-33*

17.1.1 address

DHCP Config Commands

Specifies a range of addresses for the DHCP network pool

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
address range <low IP address> <high IP address>
```

Parameters

range <low IP address> <high IP address>	Adds an address range for the DHCP server • low IP address – Defines the first IP address in the address range • high IP address – Defines the last IP address in the address range

Usage Guidelines

Use the `address` command to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address, and a low IP address is the lower limit for providing the IP address.

Use the `no address range` command to remove the DHCP address range.

Example

```
RFSwitch(config-dhcp)#address range 2.2.2.2 2.2.2.50
RFSwitch(config-dhcp)#
```

17.1.2 bootfile

DHCP Config Commands

Assigns a bootfile name for the DHCP configuration on the network pool

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
bootfile <FILE>
```

Parameters

bootfile <FILE>	Sets the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use {`no`} `bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no] bootfile` removes the existing command from the pool.

Example

```
RFSwitch(config-dhcp)#bootfile bootexample.txt
RFSwitch(config-dhcp)#
```

17.1.3 class

DHCP Config Commands

Associates a DHCP class with a pool

This command is used in Step 4 of *Creating a DHCP User Class*.

The CLI prompt moves to a sub-instance`(config-dhcp-class)`.The configuration mode changes from `(config-dhcp)# class` to `(config-dhcp-class)`.
Refer to *config-dhcp-class on page 17-7* for a `(config-dhcp-class)` command summary.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
class <class-name>
```

Parameters

class <class -name>	Associates a class with a pool and enters the DHCP pool class configuration mode

Example

```
RFSwitch(config-dhcp)#class RFS7000DHCPclass
RFSwitch(config-dhcpclass)#
```

17.1.3.1 Creating a DHCP User Class

Follow the steps below to create a DHCP User Class:

1. Create a DHCP class named **`RFSwitchDHCPclass`**. The switch supports a maximum of 32 DHCP classes.

   ```
   RFSwitch(config)#ip dhcp class RFS7000DHCPclass
   RFSwitch(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The mode changes to `(config-dhcpclass)`. The switch supports a maximum of 8 users classes per DHCP class.

   ```
   RFSwitch(config-dhcpclass)#option user-class MC800
   RFSwitch(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode.

   ```
   RFSwitch(config)#ip dhcp pool WID
   RFSwitch(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of 8 DHCP classes with a pool.

   ```
   RFSwitch(config-dhcp)#class RFS7000DHCPclass
   RFSwitch(config-dhcp-class)#
   ```

5. The switch moves to a new mode (config-dhcp-class). Use this mode to add an address range used for the DHCP class associated with the pool.

   ```
   RFSwitch(config-dhcp-class)#address range 11.22.33.44
   ```

17.1.3.2 config-dhcp-class

Use `(config-dhcp)# class` to enter the (**`config-dhcp-class) instance`**. Use this instance to set an address range for a DHCP user class within a DHCP server address pool.

Table 17.2 summarizes **`config-dhcp-class`** commands.

Table 17.2 DHCP Server Class Command Summary

Command	*Description*
address	Sets an address range for a DHCP class in a DHCP server address pool
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system in HTML format
no	Negates a command or sets its defaults
service	Assists in troubleshooting or debugging issues
show	Displays running system information

address

config-dhcp-class

Sets an address range for a DHCP class within a DHCP server address pool

Syntax

```
address range <low IP Address> <high IP Address>
```

Parameters

range <low IP Address> <high IP Address>	Assigns an address range for the DHCP class • <low IP Address> – Defines the low IP address • <high IP Address> – Defines the high IP address

Example

```
RFSwitch(config-dhcp-class)#address range 11.22.13.14
11.22.33.56
RFSwitch(config-dhcp-class)#
```

17.1.4 client-identifier

DHCP Config Commands

Assigns a name to the client-identifier

A client identifier is used to reserve an IP address for a DHCP client.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
client-identifier <identifier>
```

Parameters

client-identifier <identifier>	Prepends a null character. Use `\\0` at the beginning (a single `\` in the input is ignored)

Example

```
RFSwitch(config-dhcp)#client-identifier testid
RFSwitch(config-dhcp)#
```

17.1.5 client-name

DHCP Config Commands

Adds name for DHCP clients

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
client-name <name>
```

Parameters

client-name <name>	Use `client-name` to add a client name (the domain name must not be included)

Example

```
RFSwitch(config-dhcp)#client-name testpc
RFSwitch(config-dhcp)#
```

17.1.6 clrscr

DHCP Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-dhcp)#clrscr
RFSwitch(config-dhcp)#
```

17.1.7 ddns

DHCP Config Commands

Sets dynamic DNS parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ddns [domainname|multiple-user-class|server|ttl]

ddns domainname <name>
ddns multiple-user-class
ddns server <IP Address>
ddns ttl <1-864000>
```

Parameters

domainname <name>	Sets the domain name used for DDNS updates
multiple-user-class	Enables the multiple user class option
server <IP >	Specifies the server to which DDNS updates have been sent • <IP> – Defines an IP address in dotted decimal format
ttl <1-864000>	Sets a *Time To Live* (TTL) value for DDNS updates • <1-864000> – TTL value in seconds

Usage Guidelines

Use `update dns override` to enable an internal DHCP server to send DDNS updates for resource records (RRs) A, TXT and PTR. A DHCP server can always override the client even if the client is configured to perform the updates.

In the DHCP server network pool, FQDN is defined as the DDNS domain name. This is used internally in DHCP packets between the DHCP server on the switch and the DNS server.

Example

```
RFSwitch(config-dhcp)#ddns domainname TestDomain.com
RFSwitch(config-dhcp)#

RFSwitch(config-dhcp)#ddns multiple-user-class
RFSwitch(config-dhcp)#

RFSwitch(config-dhcp)#ddns ttl 1000
RFSwitch(config-dhcp)#
```

17.1.8 default-router

DHCP Config Commands

Configures the default router or gateway IP address for the network pool. To remove the default router list, use the `no default-router` command.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
default-router <IP>
```

Parameters

default-router < IP>	Specifies the default router IP address for the network pool • < IP> – Sets the router's IP address

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
RFSwitch(config-dhcp)#default-router 2.2.2.1
RFSwitch(config-dhcp)#
```

17.1.9 dns-server

DHCP Config Commands

Sets the DNS server's IP address available to all DHCP clients connected to the pool. Use the `no dns-server` command to remove the DNS server list.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
dns-server <IP address>
```

Parameters

dns-server <IP address>	Configures the DNS server's IP address • <IP address> – Sets the server's IP address. Up to 8 IPs can be set.

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Example

```
RFSwitch(config-dhcp)#dns-server 2.2.2.222
RFSwitch(config-dhcp)#
```

17.1.10 domain-name

DHCP Config Commands

Sets the domain name for the network pool. Use the `no domain-name` command to remove the domain name.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
domain-name <name>
```

Parameters

domain-name <name>	Defines the domain name for the network pool

Usage Guidelines

The domain name cannot exceed 256 characters.

Example

```
RFSwitch(config-dhcp)#domain-name Engineering
RFSwitch(config-dhcp)#
```

17.1.11 end

DHCP Config Commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-dhcp)#end
RFSwitch#
```

17.1.12 exit

DHCP Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch#(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config)#ip dhcp pool TestPool
RFSwitch(config-dhcp)#exit
RFSwitch(config)#
```

17.1.13 hardware-address

DHCP Config Commands

Reserves an IP address (manually) based on a DHCP client's hardware address. Use the `no hardware-address` command to remove this from the DHCP pool.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
hardware-address <MAC> {[ethernet|token-ring]}
```

Parameters

hardware-address <MAC> {ethernet|token-ring}	Sets the client's hardware address to <MAC>. <MAC> can be in the format xx-xx-xx-xx-xx-xx (dashed hexadecimal string) or XX:XX:XX:XX:XX:XX (dotted hexadecimal string) • <MAC> {ethernet|token-ring} – Defines a dashed hexadecimal string • <MAC> {ethernet|token-ring} – Sets a dotted hexadecimal string. • ethernet – Ethernet • token-ring – Token ring network

Usage Guidelines

Accepts only hexadecimal values

Example

```
RFSwitch(config-dhcp)#hardware-address 00:01:23:45:32:22
RFSwitch(config-dhcp)#
```

17.1.14 help

DHCP Config Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-dhcp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-dhcp)#
```

17.1.15 host

DHCP Config Commands

Defines a fixed IP address for the host in dotted decimal format

Use the `no host` command to remove the host from the DHCP pool.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
host <IP>
```

Parameters

host <IP>	Sets a fixed address for the host • <IP > – Sets an IP address in dotted decimal format

Usage Guidelines

The DHCP host pool (used to manually assign an IP address based on hardware address/ client identifier) configuration must contain a host IP address, client name and hardware address/client identifier.

The host IP address must belong to a subnet on the switch. There must be a DHCP network pool corresponding to that host IP address. There is no limit to the number of manual bindings. However, you can configure only one manual binding per host pool.

Example

```
RFSwitch(config-dhcp)#host 2.2.2.111
RFSwitch(config-dhcp)#
```

17.1.16 lease

DHCP Config Commands

Sets a valid lease time for the IP address used by DHCP clients in the network pool

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
lease [{<0-365> <0-23> <0-59>}|infinite]
```

Parameters

lease [{<0-365> <0-23> <0-59>} |infinite]	Sets the lease time for an IP address • <0-365> –Sets the lease period in days. Days can be made as 0 only when hours and/or mins are greater than 0. • <0-23> – Sets the hours for the lease period. Hours can be 0 only when days and/or minutes are configured with a value greater than 0. • <0-59> – Sets the minutes for the lease period. Minutes can be 0 only when days and/or hours are configured with a value greater than 0. • infinite – Sets the lease period as infinite.

Usage Guidelines

If lease parameter is not configured on the DHCP network pool, the default value is used. The default value of the lease is 24 hours.

The lease value for DHCP host pool is infinite. Hence the lease configuration is not applicable for DHCP host pool



NOTE: The factory default lease period for a pool – network pool or host pool is configured as 1 day.

Example

```
RFSwitch(config-dhcp)#lease 1 0 0
RFSwitch(config-dhcp)#
```

```
RFSwitch(config)#show running-config
.....................................
.....................................
.....................................
ip dhcp pool Test4lease
 host 3.33.33.3
 client-name test4lease
 client-identifier tested4lease
.....................................
.....................................
RFSwitch(config)#
```

```
RFSwitch(config)#show running-config include-factory
.....................................
ip dhcp pool Test4lease
 lease 1 0 0
 no domain-name
 no bootfile
 no dns-server
 no default-router
 no next-server
 no netbios-name-server
 no netbios-node-type
 no unicast-enable
 no update dns
 no ddns domainname
 no ddns ttl
 no ddns multiple-user-class
 host 3.33.33.3
 client-name test4lease
 client-identifier tested4lease
 no hardware-address
.....................................
RFSwitch(config)#
```

17.1.17 netbios-name-server

DHCP Config Commands

Sets the netbios-name server's IP address

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
netbios-name-server <IP>
```

Parameters

netbios-name-server <IP>	Defines the NetBIOS (WINS) name server • <IP > – Sets the NetBIOS name server's IP address

Example

```
RFSwitch(config-dhcp)#netbios-name-server 2.2.2.222
RFSwitch(config-dhcp)#
```

17.1.18 netbios-node-type

DHCP Config Commands

Defines the netbios-node type

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

netbios-node-type [b-node | h-node | m-node | p-node]	Defines the NetBIOS (WINS) name servers • b-node – Broadcast node • h-node – Hybrid node • m-node – Mixed node • p-node – Peer-to-peer node

Example

```
RFSwitch(config-dhcp)#netbios-node-type p-node
RFSwitch(config-dhcp)#
```

17.1.19 network

DHCP Config Commands

Sets the network pool's IP address

This address maps the current DHCP pool with a specific network.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
network [<IP>|<IP/Mask>]
```

Parameters

network [<IP>|<IP/Mask>]	Sets the network number and mask • <IP> – Network number in dotted decimal format • <IP/Mask> – Network number and mask

Usage Guidelines

Ensure a VLAN interface (with specific network/subnet) exists on the switch before mapping a DHCP pool to a particular network.

Example

```
RFSwitch(config-dhcp)#network  2.2.2.0/24
RFSwitch(config-dhcp)#
```

17.1.20 next-server

DHCP Config Commands

Sets the IP address of the next server in the boot process

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
next-server <IP>
```

Parameters

next-server <IP>	Sets the next server in boot process • <IP> – Defines the server's IP address

Example

```
RFSwitch(config-dhcp)#next-server 2.2.2.22
RFSwitch(config-dhcp)#
```

17.1.21 no

DHCP Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [address|bootfile|class|client-identifier|client-name|
ddns|default-router|dns-server|domain-name|hardware-address|
host|lease|netbios-name-server|netbios-node-type|network|
next-server|option|update|unicast-table]
```

Parameters

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFSwitch(config)#no ip dhcp pool hotpool
RFSwitch(config)#

RFSwitch(config)#no ip dhcp pool test
RFSwitch(config)#

RFSwitch(config-dhcp)#no update dns
RFSwitch(config-dhcp)#
```

17.1.22 option

DHCP Config Commands

Defines the DHCP option used in DHCP pools

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
option <option-name> [<IP>|<option-name>]
```

Parameters

option name [<IP>| <option-name>]	Sets raw DHCP options • <option-name> – Sets the name of the DHCP option • <IP> – Sets the IP value of the DHCP option • <option-name> – Sets the ASCII value of the DHCP option

Usage Guidelines

Defines non standard DHCP option codes (0-254)



NOTE: An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use double backslash to represent a single backslash.

Example

```
RFSwitch(config)#ip dhcp option option189 189 ascii
RFSwitch(config)#
```

17.1.23 service

DHCP Config Commands

Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

show cli	Displays the CLI tree of the current mode

Example

```
RFSwitch(config-dhcp)#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-class
  +-WORD [class WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
  +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
.........................
.....................................................
RFSwitch(config-dhcp)#
```

17.1.24 show

DHCP Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000: port-channel

- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-dhcp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
 environment           show environmental information
  file                  Display filesystem information
```

```
  firewall                Wireless firewall
  ftp                     Display FTP Server configuration
  history                 Display the session command history
  interfaces              Interface status
  ip                      Internet Protocol (IP)
  ldap                    LDAP server
  licenses                Show any installed licenses
  logging                 Show logging configuration and
buffer
  mac                     Internet Protocol (IP)
  mac-address-table       Display MAC address table
  mac-name                Displays the configured mac names
  management              Display L3 Managment Interface name
  mobility                Display Mobility parameters
  ntp                     Network time protocol
  password-encryption     password encryption
  port                    Physical/Aggregate port interface
  port-channel            Portchannel commands
  privilege               Show current privilege level
  radius                  RADIUS configuration commands
  redundancy              Display redundancy group parameters
    rtls                    Real Time Locating System commands
  role                    Configure role parameters
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open
connections
  smtp-notification       Display SNMP engine parameters
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group    static channel group membership
  terminal                Display terminal configuration
parameters
  timezone                Display timezone
  traffic-shape           Display traffic shaping
  upgrade-status          Display last image upgrade status
  users                   Display information about currently
logged                                in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl

RFSwitch(config-dhcp)#
```

17.1.25 update

DHCP Config Commands

Controls the usage of the DDNS service

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
update dns override
```

Parameters

update dns override	Controls the usage of the DDNS service • dns override – Dynamic DNS Configuration • override – Enable Dynamic Updates by onboard DHCP Server

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP Server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can override the client, even if the client is configured to perform the updates.

In the network pool of DHCP Server, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the switch's DHCP Server and the DNS server.

Example

```
RFSwitch(config-dhcp)#update dns override
RFSwitch(config-dhcp)#
```

17.1.26 unitcast-enable

DHCP Config Commands

Enables unicast for DHCP offer and DHCP Ack

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
unicast-enable
```

Parameters

```
None
```

Example

```
RFSwitch(config-dhcp)#unicast-enable
RFSwitch(config-dhcp)#
```

17.2 Configuring the DHCP Server using Switch CLI

The switch DHCP configuration is conducted by creating pools and mapping them to L3 interfaces (SVI).

- A Network pool is the pool with "include" ranges. When the network pool is mapped to a L3 interface, DHCP clients requesting IPs from the L3 interface get an IP from the configured range.
- A host pool is the pool used to assign static/fixed IP address to DHCP clients.

17.2.1 Creating network pool

To create a network pool:

1. Create a DHCP server dynamic address pool.

   ```
   RFSwitch(config)#ip dhcp pool test
   ```

2. Map the DHCP pool to the network pool.

   ```
   RFSwitch(config-dhcp)#network 192.168.0.0/24
   ```

3. Add the address range for the dynamic pool.

   ```
   RFSwitch(config-dhcp)#address range 192.168.0.30 192.168.0.60
   ```

4. Assign a domain name (as appropriate) to this dynamic pool.

   ```
   RFSwitch(config-dhcp)#domain-name test.com
   ```

5. Configure the DNS server's IP address.

   ```
   RFSwitch(config-dhcp)#dns-server 192.168.0.10 192.168.0.11
   ```

6. Configure the DHCP client's IP address lease period.

   ```
   RFSwitch(config-dhcp)#lease 10
   ```

7. Exit from the DHCP instance upon creation of the network pool.

   ```
   RFSwitch(config-dhcp)#exit
   ```

8. Start the DHCP server to initiate the network pool.

   ```
   RFSwitch(config)#service dhcp
   ```

17.2.2 Creating a Host Pool

To create a host pool:

1. Create a DHCP server host address pool.

   ```
   RFSwitch(config)#ip dhcp pool hostpool
   ```

2. Assign the client name of the host for which static allocation is required.

   ```
   RFSwitch(config-dhcp)#client-name linuxbox
   ```

3. Assign an IP address for the host.

   ```
   RFSwitch(config-dhcp)#host 192.168.0.50
   ```

4. Configure the hardware address of the host.

   ```
   RFSwitch(config-dhcp)#hardware 00:a0:f8:6f:6b:88
   ```

5. Exit from the DHCP instance upon creation of the network pool.

   ```
   RFSwitch(config-dhcp)#exit
   ```

6. Start the DHCP Server to instantiate the network pool.

   ```
   RFSwitch(config)#service dhcp
   ```

17.2.3 Troubleshooting DHCP Configuration

1. The DHCP Server is disabled by default. Use the following command to enable the DHCP Server:

   ```
   RFSwitch(config)#service dhcp
   ```

   This command administratively enables the DHCP server. If the DHCP configuration is incomplete, it is possible the DHCP server will be disabled even after the execution of this command.

2. Use the **`network`** command to map the network pool to interface.

   ```
   network 192.168.0.0/24
   ```

   In the above example, 192.168.0.0/24 represents the L3 interface. When you execute this command, no check is performed to endorse whether an interface (with the specified IP/Netmask) exists. The verification is not performed because you can create a pool and map it to non existing L3 interface.

   When you add a L3 interface and assign an IP address to it, the DHCP server gets enabled/started on this interface. If you have a pool for network 192.168.0.0/24, but the L3 interface is 192.168.0.0/16, DHCP is not enabled on 192.168.0.0/16, since it is different from 192.168.0.0/24.

3. A network pool without any include range is as good as not having a pool. Add a include range using the **`address range`** command.

   ```
   address range 192.168.0.30 192.168.0.30
   ```

4. To work properly, a host pool should have the following 3 items configured:

   - client-name (CLI is **`client-name <name>`**)
   - fixed-address CLI is **`host <ip>`**)
   - hardware-address/client-identifier

   The hardware address is **`hardware-address <addr>`**

   The client-identifier is **`client-identifier <id>`**

   If you use **`client-identifier`** instead of **`hardware-address`**, a DHCP client sends the client-identifier when it requests for IP address. The Client - identifier has to be configured in the DHCP Client as an ASCII value and the same has to be used in the DHCP server option (for example, the Client- identifier option).

5. A host pool should have its corresponding network pool configured, otherwise the host pool is useless. The fixed IP address configured in the host pool must be in the subnet of the corresponding network pool.
6. If you create a pool and map it to an interface, it automatically gets enabled, provided DHCP is enabled at a global level. Use the **`no network`** command to disable DHCP on a per pool/interface basis.
7. To set a newly created pool as a network pool, use one of the following commands:
   - **`network (for example, network 192.168.0.0/24)`**
   - **`address range (for example, address range 192.168.0.30 192.168.0.50)`**
8. To set a newly created pool as a host pool, use one of the following commands:
   - **`host (for example, host 192.168.0.1)`**
   - **`client-name (For example, client-name "MailUsers")`**
   - **`client-identifier (For example, client-identifier "aabb:ccdd")`**
   - **`hardware-address (For example, hardware-address “aa:bb:cc:dd:ee:ff”)`**
9. A pool can be configured either as the host pool or network pool, but not both.
10. A host pool can have either **`client-identifier`** or **`hardware-address`** configured, but not both.
11. An excluded address range has a higher precedence than an included address range. Thus, if a range is part of both an excluded and included range, it will be excluded.
12. DHCP options are first defined at the global level using **`ip dhcp option <name> <code> <type>`**. The value for these options are defined using the **`option`** under the DHCP pool context.

17.2.4 Creating a DHCP Option

To create a DHCP option:

1. To create a non standard option named “tftp-server”.

   ```
   RFSwitch(config)#ip dhcp option tftp-server 183 ip
   ```

2. Enter the DHCP pool —”test”.

   ```
   RFSwitch(config)#ip dhcp pool test
   ```

3. Assign a value to the DHCP option configured above.

   ```
   RFSwitch(config-dhcp)#option tftp-server 192.168.0.100
   ```

4. Exit the DHCP instance.

   ```
   RFSwitch(config-dhcp)#exit
   ```

18

DHCP Class Instance

Use the (config-dhcpclass) instance to configure DHCP user classes. The switch supports a maximum of 8 user classes per DHCP class. To navigate to this instance use the command:

```
RFSwitch(config)#ip dhcp class <class-name>
RFSwitch(config-dhcpclass)#
```

Refer to *ip on page 12-10* and *DHCP Class Instance on page 18-1* for other DHCP related configurations.

18.1 DHCP Server Class Config Commands

Table 18.1 summarizes `config-std-nacl` commands:

Table 18.1 DHCP Server Class Config Commands

Command	Description	Ref.
clrscr	Clears the display screen	*page 18-3*
end	Ends the current mode and moves to the EXEC mode	*page 18-4*
exit	Ends the current mode and moves to the previous mode	*page 18-5*
help	Displays the interactive help system in HTML format	*page 18-6*
multiple-user-class	Enables multiple user class options	*page 18-7*

Table 18.1 DHCP Server Class Config Commands

Command	***Description***	***Ref.***
no	Negates a command or sets its defaults	*page 18-8*
option	Defines DHCP Server options	*page 18-9*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 18-11*
show	Displays running system information	*page 18-12*

18.1.1 clrscr

DHCP Server Class Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#clrscr
RFSwitch(config-dhcpclass)#
```

18.1.2 end

DHCP Server Class Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

end

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#end
RFSwitch#
```

18.1.3 exit

DHCP Server Class Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#exit
RFSwitch(config)#
```

18.1.4 help

DHCP Server Class Config Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-dhcpclass)#
```

18.1.5 multiple-user-class

DHCP Server Class Config Commands

Enables the multiple-user-class option

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
multiple-user-class
```

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#multiple-user-class
RFSwitch(config-dhcpclass)#
```

18.1.6 no

DHCP Server Class Config Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [multiple-user-class|option]
np option user-class <class-name>
```

Parameters

multiple-user-class	Disables the multiple user class option
option user-class <class-name>	Modifies the parameters of existing DHCP server options • user-class <class-name> – Configures DHCP-Server user class options • <class-name> – ASCII value of user-class option

Example

```
RFSwitch(config-dhcpclass)#no multiple-user-class
RFSwitch(config-dhcpclass)#
```

18.1.7 option

DHCP Server Class Config Commands

Specifies a value for DHCP user class options

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
option user-class <class-name>
```

Parameters

user-class <class-name>	Creates/modifies DHCP server user class options • <class-name> – ASCII value of user-class option

Example

```
RFSwitch(config-dhcpclass)#option user-class MC800
RFSwitch(config-dhcpclass)#
```

18.1.7.1 Creating a DHCP User Class

Complete the steps below to create a DHCP user class:

1. Create a DHCP class named **`RFS7000DHCPclass`**. The switch supports a maximum of 32 DHCP classes.

   ```
   RFSwitch(config)#ip dhcp class RFS7000DHCPclass
   RFSwitch(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. The switch supports a maximum of 8 user classes per DHCP class.

   ```
   RFSwitch(config-dhcpclass)#option user-class MC800
   RFSwitch(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using the `(config)#` mode.

   ```
   RFSwitch(config)#ip dhcp pool WID
   RFSwitch(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of 8 DHCP classes with a pool.

   ```
   RFSwitch(config-dhcp)#class RFS7000DHCPclass
   RFSwitch(config-dhcp-class)#
   ```

5. The switch moves to a new mode (config-dhcp-class). Use this mode to add an address range for the DHCP class associated with the pool.

   ```
   RFSwitch(config-dhcp-class)#address range 11.22.33.44
   ```

18.1.8 service

DHCP Server Class Config Commands

Invokes service commands to troubleshoot or debug (config-if) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-dhcpclass)#service show cli
DHCP Server Class Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-multiple-user-class [multiple-user-class_cmd]
+-no
  +-multiple-user-class [no multiple-user-class_cmd]
  +-option
    +-user-class
      +-WORD [no option user-class WORD]
+-option
  +-user-class
    +-WORD [option user-class WORD]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
.....................................................
......
.....................................................
.......RFSwitch(config-dhcpclass)#
```

18.1.9 show

DHCP Server Class Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-dhcpclass)#show ?
 access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
```

```
  dhcp                    DHCP Server Configuration
 environment             show environmental information
  file                    Display filesystem information
  firewall                Wireless firewall
  ftp                     Display FTP Server configuration
  history                 Display the session command history
  interfaces              Interface status
  ip                      Internet Protocol (IP)
  ldap                    LDAP server
  licenses                Show any installed licenses
  logging                 Show logging configuration and
buffer
  mac                     Internet Protocol (IP)
  mac-address-table       Display MAC address table
  mac-name                Display the configured MAC names
  management              Display L3 Managment Interface name
  mobility                Display Mobility parameters
  ntp                     Network time protocol
  password-encryption     password encryption
  port                     Physical/Aggregate port interface
  port-channel            Portchannel commands
  privilege               Show current privilege level
  radius                  RADIUS configuration commands
  redundancy      Display redundancy group parameters
  role                   Configure role parameters
  rtls                    Real Time Locating System commands
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open
connections
  smtp-notification      Display SNMP engine parameters
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group   static channel group membership
  traffic-shape          Display traffic shaping
  terminal                Display terminal configuration
parameters
  timezone                Display timezone
  upgrade-status          Display last image upgrade status
  users                   Display information about currently
logged                           in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
```

```
  wlan-acl              wlan based acl

RFSwitch(config-dhcpclass)#show

RFSwitch(config-dhcpclass)#show ip dhcp binding
IP               MAC/Client-Id       Expiry Time
--               -------------       -----------
RFSwitch(config-dhcpclass)#

RFSwitch(config-dhcpclass)#show ip dhcp class
RFS7000DHCPclass
!
ip dhcp class DHCPclass
 option user-class MC800
RFSwitch(config-dhcpclass)#


RFSwitch(config-dhcpclass)#show ip dhcp pool WID
!
ip dhcp pool WID
 class RFS7000DHCPclass
  address range 11.22.33.44
RFSwitch(config-dhcpclass)#
```

19

Radius Server Instance

Use the `(config-radsrv)` instance to configure local RADIUS server parameters. Local (Onboard) RADIUS server commands are listed under this mode. To navigate to this instance, use the command:

```
RFSwitch(config)#radius-server local
RFSwitch(config-radsrv)#
```

19.1 Radius Configuration Commands

Table 19.1 summarizes the Global Config command:

Table 19.1 RADIUS Server Command Summary

Command	Description	Ref.
authentication	Configures the authentication scheme used with the RADIUS server	*page 19-3*
ca	Defines CA parameters	*page 19-5*
clrscr	Clears the display screen	*page 19-6*
crl-check	Enables a *Certificate Revocation List* (CRL) check	*page 19-7*
end	Ends the current mode and moves to the EXEC mode	*page 19-8*
exit	Ends the current mode and moves to the previous mode	*page 19-9*

Table 19.1 RADIUS Server Command Summary

Command	Description	Ref.
group	Sets RADIUS user group parameters. **NOTE:** This command navigates to another sub-instance called **`config-radsrv-group`** with its own command summary.	*page 19-10*
help	Displays the interactive help system	*page 19-23*
ldap-server	Sets LDAP server parameters	*page 19-24*
nas	Sets RADIUS client parameters	*page 19-27*
no	Negates a command or sets its defaults	*page 19-28*
proxy	Defines the RADIUS proxy server configuration	*page 19-29*
rad-user	Sets the RADIUS user configuration	*page 19-31*
server	Configures server certificate parameters	*page 19-34*
service	Invokes service commands to troubleshoot or debug **`(config-radsrv)`** instance configurations	*page 19-35*
show	Displays running system information	*page 19-36*
ldap-group-verification	Sets LDAP Group Verification	*page 19-38*

19.1.1 authentication

Radius Configuration Commands

Configures the authentication scheme used with the RADIUS server

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication eap-auth-type [all|peap-gtc|
peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

Parameters

authentication data-source [ldap|local]	Configures authentication • data-source [ldap|local] – Sets the RADIUS data source for user authentication • ldap - Remote LDAP Server • local - Local user database
eap-auth-type [all| peap-gtc| peap-mschapv2|tls| ttls-md5|ttls-mschapv2 ttls-pap]	Defines RADIUS EAP and default authentication configurations • all – Enables TTLS and PEAP settings • peap-gtc – Defines the EAP and PEAP settings used with the default authentication configuration • peap-mschapv2 – Sets the EAP/PEAP type used with mschapv2 • tls – Defines an EAP/TLS configuration scheme • ttls-md5 – Sets the EAP/TTLS configuration used with the default md5 authentication scheme • ttls-mschapv2 – Sets the EAP/TTLS configuration used with the default mschapv2 authentication scheme • ttls-pap – Sets the EAP/TTLS configuration used with the default pap authentication scheme

Usage Guidelines

Set **`eap-auth-type`** to **`all`** to service RADIUS requests received from mobile units. Setting `eap-auth-type` to `peap-gtc/peap-mschapv2` ensures `peap-gtc/peap-mschapv2` service only.

Similarly, setting `eap-auth-type` to `ttls-md5/ttls-mschapv2/ttls-pap` services all ttls authentication requests from mobile units.

Setting `eap-auth-type` to `tls` ensures only tls authentication is serviced.

Example

```
RFSwitch(config-radsrv)#authentication eap-auth-type peap-
mschapv2
RFSwitch(config-radsrv)#

RFSwitch(config-radsrv)#authentication data-source ldap
RFSwitch(config-radsrv)#
```

19.1.2 ca

Radius Configuration Commands

Configures CA (*Certificate Authority*) parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ca trust-point <trustpoint-name>
```

Parameters

trust-point <trustpoint-name>	Defines the trustpoint configuration • <trustpoint-name> – Displays the existing trustpoint name

Usage Guidelines

Configures the trustpoint used by the local RADIUS server. Create the **`trustpoint`** before it can be used by the **`crypto pki trustpoint`** command.

The default trust point in use is – `default-trustpoint`.

Example

```
RFSwitch(config)#radius-server local
RFSwitch(config-radsrv)#ca trust-point tp1
RFSwitch(config-radsrv)#
```

19.1.3 clrscr

Radius Configuration Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-radsrv)#clrscr
RFSwitch(config-radsrv)#
```

19.1.4 crl-check

Radius Configuration Commands

Enables a *Certificate Revocation List* (CRL) check

To enable the certificate revocation list, ensure the `crl list` is loaded using a `crypto pki import <trustpoint-name> crl` command.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
crl-check enable
```

Parameters

enable	Enables the CRL check

Usage Guidelines

TLS uses certificates for authentication. CRL (updated with a trustpoint), contains index numbers of revoked certificates. The CRL checks for any revoked certificates used for `tls` authentication.

Example

```
RFSwitch(config-radsrv)#crl-check enable
RFSwitch(config-radsrv)#
```

19.1.5 end

Radius Configuration Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-radsrv)#end
RFSwitch#
```

19.1.6 exit

Radius Configuration Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-radsrv)#exit
RFSwitch(config)#
```

19.1.7 group

Radius Configuration Commands

Configures RADIUS user groups

The CLI moves to the `config-radsrv-group` sub-instance to create a new group.

The prompt changes from `RFSwitch(config-radsrv)#` to `RFSwitch(config-radsrv-group)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Table 19.2 summarizes the RADIUS user group commands within the **`(config-radsrv-group)`** sub-instance.

Table 19.2 RADIUS User Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 19-11*
end	Ends the current mode and moves to the EXEC mode	*page 19-11*
exit	Ends the current mode and moves to the previous mode	*page 19-11*
group	Sets RADIUS user group parameters	*page 19-12*
guest-group	Defines guest group permissions	*page 19-12*
help	Displays the interactive help system in HTML format	*page 19-13*
no	Negates a command or sets its defaults	*page 19-14*
policy	Defines the RADIUS group access policy configuration	*page 19-15*
rad-user	Adds a RADIUS user to this group	*page 19-17*
rate-limit	Sets rate limit for group	*page 19-17*
service	Invokes RADIUS service commands if stopped	*page 19-18*

Table 19.2 RADIUS User Group Command Summary

Command	Description	Ref.
show	Displays running system information	page 19-19

19.1.7.1 clrscr

group

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-radsrv-group)#clrscr
RFSwitch(config-radsrv-group)#
```

19.1.7.2 end

group

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to **`RFSwitch#`**

Syntax

```
end
```

Parameters

None

Example

```
RFSwitch(config-radsrv-group)#end
RFSwitch#
```

19.1.7.3 exit

group

Ends the current mode and moves to the previous mode (`config-radsrv`)). The prompt changes to **`RFSwitch(config)#`**.

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config-radsrv-group)#exit
RFSwitch(config-radsrv)#group
```

19.1.7.4 group

group

Establishes RADIUS user group parameters. This command creates a group within the existing RADIUS group

Syntax

```
group <group-name>
```

Parameters

<group-name>	Defines the RADIUS group name

Example

```
RFSwitch(config-radsrv-group)#group TestGroup
RFSwitch(config-radsrv-group)#
```

19.1.7.5 guest-group

group

Manages a guest user linked with a hotspot. Create a guest-user and associate it with the guest-group. The guest-user and the policies of the guest group are used for hotspot authentication/authorization.

Syntax

```
guest-group enable
```

Parameters

guest-group enable	Defines this group as a guest group

Usage Guidelines

Creates a guest group. The guest user created using `rad-user` can only be part of the guest group.

Example

```
RFSwitch(config-radsrv-group)#guest-group enable
RFSwitch(config-radsrv-group)#
```

19.1.7.6 help

group

Displays the system's interactive help in HTML format.

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-radsrv-group)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-radsrv-group)#
```

19.1.7.7 no

group

Use this command to negate a command or set its defaults

Syntax

```
no [policy|rad-user|rate-limit]
no policy [day|time|vlan|wlan]
no policy wlan [<1-256>|all] <1-256>
no rate-limit [wired-to-wireless|wireless-to-wired]
```

Parameters

policy [day|time|vlan| wlan]	Defines the RADIUS group access policy configuration • day – Resets the access policy (days of permitted access) for this group • time – Configures the group's hourly access permissions • vlan – Sets the VLAN ID for the group • wlan [<1-256>|all] – Configures WLAN access policy for this group • <1-256> – Sets the WLAN range for the access policy • all – Removes all the WLAN allowed
rad-user [<name>|all]	Removes a user from this group • <name> – Defines an existing user name in this group • all – Removes all users from this group
rate-limit [wired-to-wireless| wireless-to-wired]	Negate a command or set its defaults • wired-to-wireless –uplink direction - from wireless client to network • wireless-to-wired – down-link-direction - from network to wireless client

Example

```
RFSwitch(config-radsrv-group)#no policy day
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#no policy time
```

```
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#no policy vlan
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#no policy wlan 2 5
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#no rad-user all
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#no service radius
%%Info: Radius service stopped...
RFSwitch(config-radsrv-group)#
```

19.1.7.8 policy

▸ *group*

Sets the authorization policies for a particular group (like day/time of access, WLANs allowed etc.).



NOTE: A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN (as defined within the WLAN Configuration screen).

Syntax

```
policy [day|time|vlan|wlan]
policy day [all|su|mo|tu|we|th|fr|sa|weekdays]
policy time [start <0-23> <0-59>] [end <0-23> <0-59>]
policy vlan <1-4094>
```

Parameters

day [all|su|mo|tu|we|th|fr|sa|weekdays]	Day of access policy configuration • all – All days (from Sunday to Saturday) • su – Sunday • mo – Monday • tu – Tuesday • we – Wednesday • th – Thursday • fr – Friday • sa – Saturday • weekdays – Allows access only during weekdays (M-F)
time [start <0-23> <0-59>] [end <0-23> <0-59>]	Sets the access policy time for this group • start – Sets the start time • end – Defines the end time (must be greater than the start time) • <0-23> – Sets the hourly (hh) access limit • <0-59> – Sets the minute (mm) access limit
vlan <1-4096>	Sets the VLAN ID for this group • <1-4096> – Defines the VLAN range
wlan <1-256>	Sets the WLAN access policy for this group • <1-256> – Sets the WLAN index

Example

```
RFSwitch(config-radsrv-group)#policy day weekdays
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#policy time start 12 12 end 22
22
RFSwitch(config-radsrv-group)#

RFSwitch(config-radsrv-group)#policy vlan 20
RFSwitch(config-radsrv-group)#
```

```
RFSwitch(config-radsrv-group)#policy wlan 20 21 22 23
RFSwitch(config-radsrv-group)#
```

19.1.7.9 rad-user

Radius Configuration Commands

Adds an existing RADIUS user to this group. If the RADIUS user is not available in the Onboard RADIUS server's database, create a new RADIUS user using the `rad-user` command from within the `(config-radsrv)` mode.
For more information, see *rad-user on page 19-31*.

Syntax

```
rad-user <name>
```

Parameters

<name>	Existing RADIUS user name

Example

```
RFSwitch(config-radsrv)#rad-user user1 password user1
RFSwitch(config-radsrv)#group group1
RFSwitch(config-radsrv-group)#rad-user user1
RFSwitch(config-radsrv-group)#
```

19.1.7.10 rate-limit

Radius Configuration Commands

Sets the rate limit for the RADIUS Server group

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired ]
<100-100000>
```

Parameters

wired-to-wireless <100-100000>	Down link direction from network to wireless client • <100-100000> – Rate in the range of <100-100000> kbps

wireless-to-wired <100-100000>	Up link direction from wireless client to network • <100-100000> – Rate in the range of <100-100000> kbps

Usage Guidelines

Use `[no] rate-limit [wired-to-wireless|wireless-to-wired]`to remove the rate limit applied to the group.

`[no] rate-limit [wireless-to-wired]` sets the rate limit back to unlimited

Example

```
RFS6000(config-radsrv-group)#rate-limit wired-to-wireless
100
RFS6000(config-radsrv-group)#

RFS6000(config-radsrv-group)#rate-limit wireless-to-wired
1000
RFS6000(config-radsrv-group)#
```

19.1.7.11 service

Radius Configuration Commands

Invokes RADIUS service commands (if they have been stopped). This command enables the RADIUS server. A RADIUS restart is executed only from the `config` mode.

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-radsrv-group)#service show cli
Radius user group configuration mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-group
  +-WORD [group WORD]
+-guest-group
```

```
  +-enable [guest-group enable]
+-help [help]
.....................................................
.....................................................
.....................................................
.....................
RFSwitch(config-radsrv-group)#
```

19.1.7.12 show

Radius Configuration Commands

Displays current system information running on the switch

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-radsrv-group)#show ?
  access-list          Internet Protocol (IP)
  aclstats             Show ACL Statistics information
  alarm-log            Display all alarms currently in the
system
  arpi                 ARPI Configuration
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login
banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               encryption module
  debugging            Debugging information outputs
  dhcp                 DHCP Server Configuration
  environment          show environmental information
  espi                 ESPI Configuration
  file                 Display filesystem information
  firewall              Wireless firwall
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status
```

```
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-name               Displays the co nfigured MAC names
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  power                 show power over ethernet command
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy    Display redundancy group parameters
  redundancy-history    Display state transition history of
  role                   Configure role parameters
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
  smtp-notifications     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  tags                  Tags/Assets (passive, active, wi-fi,
uwb)                         Information
  static-channel-group Display static channel group
membership
  terminal              Display terminal configuration
parameters
  timezone              Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently
logged                         in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFSwitch(config-radsrv-group)#
```

19.1.7.13 Example–Creating a Group

The **(config-radsrv-group)** sub-instance is explained in the example below:

1. Create a group called Sales in the local RADIUS server database.
   RFSwitch(config-radsrv)#group sales
2. Check the RADIUS user group's configuration.

   ```
   RFSwitch(config-radsrv-group)#?
   RADIUS user group configuration commands:
   ```

3. Use a **policy** command to configure group policies for the group created in Step 1.

   ```
   RFSwitch(config-radsrv-group)#policy ?
   day   Day of access policy configuration
   time  Configure time of access policy for this group
   vlan  VLAN id for this group
   wlan  Configure wlan access policy for this group

   RFSwitch(config-radsrv-group)#policy day weekdays
   RFSwitch(config-radsrv-group)#policy time start 12 30 end 15 30
   ```

4. Use the **policy vlan** command to assign a VLAN ID of 10 to the Sales group.
   RFSwitch(config-radsrv-group)#policy vlan 10
5. Use the **policy wlan** command to allow only authorized users to access this group's WLAN.
   RFSwitch(config-radsrv-group)#policy wlan 1 2 5
6. Use **(config-radsrv)#rad-user** to create a user called **testuser** and add it to the group.

   ```
   RFSwitch(config-radsrv)#rad-user testuser password testpassword
   group sales
   Mar 07 17:41:55 2008: RADCONF: Adding user "testuser" into local
   database
   Mar 07 17:41:55 2008: RADCONF: User "testuser" is added to group
   "sales"
   ```

7. Use **(config-radsrv)#nas** to add a NAS entry for the group.

   ```
   RFSwitch(config-radsrv)#nas ?
   A.B.C.D/M  Radius client IP address

   RFSwitch(config-radsrv)#nas 10.10.10.0/24 ?
   ```

```
key  Radius client shared secret

RFSwitch(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

RFSwitch(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

8. Use **(config-radsrv)#proxy** to add a realm name for the group.
   RFSwitch(config-radsrv)#proxy realm mydomain.com server 10.10.1.10 port 1812 secret 0 testing
9. Save the changes and restart the RADIUS server.

```
RFSwitch(config-radsrv)#service radius restart
Mar 07 17:48:04 2006: %PM-5-PROCSTOP: Process "radiusd" has been
stopped
Mar 07 17:48:05 2006: RADCONF: radius config files generated
successfully
RFSwitch(config-radsrv)#Mar 07 17:48:05 2006: %DAEMON-6-INFO:
radiusd[8830]: Ready to process requests.
```

19.1.8 help

Radius Configuration Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-radsrv)#help?
  help  Description of the interactive help system

RFSwitch(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-radsrv)#
```

19.1.9 ldap-server

Radius Configuration Commands

Sets the LDAP server configuration

It uses the existing external database (active directory with the onboard RADIUS server) instead of the local database on the switch.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ldap-server [primary|secondary] host <IP>

ldap-server primary host <IP> port <1-65535>
login <user-name> bind-dn <distinguished-name> base-dn
<distinguished-name> passwd {<password>|<password>
|<password>} passwd-attr <password-attribute>
group-attr <group-attribute> group-filter
<group-filter> group-membership <group> net-timeout <1-10>

ldap-server secondary host <IP> port <1-65535> login <user-
name> bind-dn <distinguished-name> base-dn <distinguished-
name> passwd {<password>|<password>|
<password>} passwd-attr <password-attribute>
group-attr <group-attribute> group-filter <group-filter>
group-membership <group> net-timeout <1-10>
```

Parameters

ldap-server primary host <IP> port <1-65535> login <user-name> bind-dn <distinguished-name> base-dn <distinguished-name> passwd {<password>|<password>|<password>} passwd-attr <password-attribute> group-attr <group-attribute> group-filter <group-filter> group-membership <group> net-timeout <1-10>	Sets the primary LDAP server's configuration • host < IP> – Sets the LDAP server's IP configuration • <IP> – Defines the LDAP server IP address • port <number> – Enter the TCP/IP port number for the LDAP server acting as the data source • login <user-name> – Use the following as the login: `(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})` • bind-dn <distinguished-name> – Specifies the distinguished name to bind with the LDAP server • base-dn <distinguished-name> – Specifies a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. • passwd {<password>|<password>|<password>} – Sets a valid password for the LDAP server • passwd-attr <password-attribute> – Enter the password attribute used by the LDAP server for authentication • group-attr <group-attribute> – Specifies the group attribute used by the LDAP server • group-filter <group-filter> – Specifies the group filters used by the LDAP server • group-membership <group> – Specifies the Group Member Attribute sent to the LDAP server when authenticating users • net-timeout<1-10> – Enter a timeout the system uses to terminate the connection to the RADIUS Server if no activity is detected

ldap-server secondary host <IP> port <1-65535> login <user-name> bind-dn <distinguished-name> base-dn <distinguished-name> passwd {<password>|<password>|<password>} passwd-attr <password-attribute> group-attr <group-attribute> group-filter <group-filter> group-membership <group> net-timeout <1-10>	Defines the secondary LDAP server's configuration.

Usage Guidelines

Use the login filter and group filter values (described in the example below) for all LDAP configuration scenarios

Use the `passwd` parameter to enter the password for the active directory user mentioned in bind -dn. This is used for the initial login to the active directory.

The `passwd-attr` and `group-membership` is retained as described in the following example:

Example

```
RFSwitch(config)#ldap-server primary host xxx.xxx.x.xx port
389 login (sAMAccountName=%{Stripped-User-Name:-%{User-
Name}}) bin
d-dn cn=admin,ou=wid,dc=symbolTech,dc=local base-dn
ou=wid,dc=symbolTech,dc=local passwd SYMBOL@123 passwd-attr
UserPassword
group-attr cn group-filter
(|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{L
dap-UserDn}))) group-membership radiusGroupName net-timeout
1
RFSwitch(config)#
```

19.1.10 nas

Radius Configuration Commands

Sets the configuration of the RADIUS client

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
nas <IP/Mask> key [0<key>|2<key>|<key>]
```

Parameters

<IP/Mask>	Sets the RADIUS client's IP address
[0<key>|2<key>|<key>]	Sets the RADIUS client's shared key • 0 – Defines the Password as UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • LINE – Defines the secret (client shared secret) up to 32 characters

Example

```
RFSwitch(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

RFSwitch(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

RFSwitch(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

RFSwitch(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

19.1.11 no

Radius Configuration Commands

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [authentication|ca|crl-check|group|ldap-server|nas|proxy|
rad-user|server]
```

Parameters

None

Example

```
RFSwitch(config-radsrv)#no authentication data-source
RFSwitch(config-radsrv)#

RFSwitch(config-radsrv)#no ca trust-point
RFSwitch(config-radsrv)#
```

19.1.12 proxy

Radius Configuration Commands

Configures a proxy RADIUS server based on the realm/suffix

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
proxy [realm|retry-count|retry-delay]
proxy relam <relam-name> server <IP> port <1024-65535>
secret{<secret>|<secret>|<secret>}
```

Parameters

relam <relam-name> server <IP> port <1024-65535> secret {<secret>|<secret>|<secret>}	The realm name is a string of up to 50 characters • server <IP> – Sets the proxy server IP address • port <1024-65535> – Sets the proxy server port number • secret {<secret>|<secret>|<secret>} – Sets the proxy server secret string • <secret> – Password is specified UNENCRYPTED • <secret> – Password is encrypted with a password encryption secret • <secret> – Sets the proxy server shared secret up to 32 characters
retry-count <3-6>	Defined the proxy server retry count value
retry-delay<5-10>	Defines the proxy server retry delay time (in seconds)

Usage Guidelines

Only five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the switch transmits each RADIUS request before giving up. The timeout value defines the duration for which the switch waits for a reply to a RADIUS request before retransmitting the request.

Example

```
RFSwitch(config-radsrv)#proxy realm Test server 10.10.10.1
port 2220 secret "Very Very Secret !!!"
RFSwitch(config-radsrv)#

RFSwitch(config-radsrv)#proxy retry-count 5
RFSwitch(config-radsrv)#

RFSwitch(config-radsrv)#proxy retry-delay 8
RFSwitch(config-radsrv)#
```

19.1.13 rad-user

Radius Configuration Commands

Sets RADIUS user parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rad-user <user-name>
rad-user <user-name> [access|password|privilege]
rad-user <user-name> access [console|ssh|telnet|web]
rad-user <user-name> password [0<password>|2<password>
|<password>] group guest expiry-time <HH:MM> expiry-date
<MM:DD:YYYY> start-time <HH:MM> start-date <MM:DD:YYYY>]
rad-user <user-name> privilege [helpdesk|monitor|
nwadmin|superuser|sysadmin|webadmin]
```

Parameters

<user-name> [access|console|ssh |telnet|web>]	Enter a user name up to 64 characters in length • access [console|ssh|telnet|web>] – Set management user access mode • console – Only allowed from console • ssh – Only allowed from ssh • telnet – Only allowed from telnet • web – Only allowed from applet

password [0<password>|2<password>|<password>] group guest expiry-time <HH:MM> expiry-date <MM:DD:YYYY> start-time <HH:MM> start-date <MM:DD:YYYY>]	Sets the RADIUS user password • 0 <password> – Defines the password as UNENCRYPTED • 2 <password> – The password is encrypted with a password encryption secret • <password> – Sets a password up to 21 characters in length • group – Radius server group configuration • <group-name> – Existing group name in local database • guest – Enable guest user access • expiry-time <HH:MM> – Time of expiry • expiry-date <MM:DD:YYYY> – Date of expiry • start-time <HH:MM> – User account activation time • start-date <MM:DD:YYYY> – User access start date

privilege [helpdesk|monitor| nwadmin|superuser| sysadmin|webadmin]	Set management user access privilege • helpdesk [monitor|nwadmin|superuser|sysadmin|webadmin]– helpdesk (troubleshooting) access • monitor [helpdesk|nwadmin|superuser|sysadmin|webadmin]– Monitor (read-only) access • nwadmin [helpdesk|monitor|superuser|sysadmin|webadmin]– Network (wired&wireless) admin access superuser[helpdesk|monitor|nwadmin|sysadmin|webadmin]– Superuser (root) access • sysadmin [helpdesk|monitor|nwadmin|superuser|webadmin] – System <general system configuration>admin access • webadmin [helpdesk|monitor|nwadmin|superuser|sysadmin]– Web auth (hotspot) user admin access

Usage Guidelines

Use `group, guest, expiry-time expiry-date, start-time` and `start-date` parameters to create a RADIUS guest user.

The RADIUS user group specified while creating a guest user must be a *guest-group*.

Example

```
RFSwitch(config-radsrv)#rad-user TestRadUser password "I SPY
U"
RFSwitch(config-radsrv)#

RFSwitch(config-radsrv)#rad-user guest1 password 0 password1
group guest-group
guest expiry-time 12:12 expiry-date 05:12:2007 start-time
12:12 start-date 05:11:2007
RFSwitch(config-radsrv)#
```

19.1.14 server

Radius Configuration Commands

Configures server certificate parameters used by a RADIUS server

The server certificate is a part of a trustpoint created using *crypto on page 5-22.*

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
server trust-point <trust-point name>
```

Parameters

server trust-point <trust-point name>	Configures server certificate parameters • trust-point <trust-point name> – Sets the trustpoint configuration • <trust-point name> – Existing trustpoint name

Usage Guidelines

Create a trustpoint using **`(crypto-pki-trustpoint)`**. The server certificate must be created under the trustpoint using crypto-pki commands. Refer to *crypto on page 5-22* for more information.

Example

```
RFSwitch(config-radsrv)#server trust-point TestTP
RFSwitch(config-radsrv)#
```

19.1.15 service

Radius Configuration Commands

Invokes the service commands to troubleshoot or debug the `(config-radsrv)` instance configuration

This command is also used to enable the RADIUS server.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-radsrv)#service show cli
Radius Configuration mode:
+-authentication
  +-data-source
    +-ldap [authentication data-source (local|ldap)]
    +-local [authentication data-source (local|ldap)]
  +-eap-auth-type
    +-all [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-peap-gtc [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-peap-mschapv2 [authentication eap-auth-type (ttls-
md5|ttls-pap|ttls-mschap
v2|peap-gtc|peap-mschapv2|tls|all)]
    +-tls [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-ttls-md5 [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-ttls-mschapv2 [authentication eap-auth-type (ttls-
md5|ttls-
```

19.1.16 show

Radius Configuration Commands

Displays current system information running on the switch

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-radsrv)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
 environment            show environmental information
  file                   Display filesystem information
  firewall              Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name              Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                  Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy              Display redundancy group parameters
  role                  Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-notifications    Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  traffic-shape         Display traffic shaping
  upgrade-status         Display last image upgrade status
  users                  Display information about currently
logged in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl
RFSwitch(config-radsrv)#show
```

19.1.17 ldap-group-verification

Radius Configuration Commands

Displays ldap group verification settings

- RFS7000
- RFS6000

Syntax

```
ldap-group-verification [disable|enable]
```

Parameters

ldap-group-verification [disable|enable]	Displays ldap group verification settings • disable – Disables group verification • enable – Enables group verification

Example

```
RFSwitch(config-radsrv)#ldap-group-verification disable
RFSwitch(config-radsrv)#
```

20

Wireless Instance

Use the `(config-wireless)` instance to configure local RADIUS server parameters associated with the switch.

To navigate to this instance, use the command from the Global Config mode.

```
RFSwitch(config)#wireless
RFSwitch(config-wireless)#
```

20.1 Wireless Configuration Commands

This table summarizes **`(config-wireless)`** commands:

Command	Description	Ref.
aap	Sets *Adaptive AP* (AAP) related commands	*page 20-5*
admission-control	Enable admission control across all radios	*page 20-7*
adopt-unconf-radio	Adopts a radio even if its not yet configured. The default templates can be used for configuration.	*page 20-8*
adoption-pref-id	Used as a preference identifier for this switch. All radios configured with this preference identifier are more likely to be adopted by this switch.	*page 20-9*
ap	Displays access port related commands	*page 20-10*

Command	Description	Ref.
ap-containment	Defines the Rogue AP containment configuration	*page 20-13*
ap-detection	Defines the AP detection configuration	*page 20-14*
ap-image	Defines the path to upload the new image over an AP	*page 20-16*
ap-ip	Modifies static IP information for access ports	*page 20-17*
ap-standby-attempts-threshold	Sets the number of attempts after which the stand-by switch starts adopting APs	*page 20-19*
ap-timeout	Changes the default inactivity timeout for access ports	*page 20-20*
ap-udp-port	Configures the UDP port for AP L3 adoption. Enable this option in the DHCP Server supporting this access-port.	*page 20-21*
auto-select-channels	Configures the channels that will be used when ACS or DFS is performed.	*page 20-22*
broadcast-tx-speed	Sets the rate at which broadcast and multicast traffic is transmitted	*page 20-23*
client	Defines the wireless client configuration	*page 20-24*
clrscr	Clears the display screen	*page 20-28*
cluster-master-support	Changes settings for cluster master support. This is required for cluster-level functions	*page 20-29*
convert-ap	Changes an AP's mode of operation	*page 20-30*
country-code	Configures the country of operation. All existing radio configurations are erased.	*page 20-33*
debug	Debugging functions.	*page 20-34*

Command	Description	Ref.
dhcp-one-portal-forward	Enables forwarding of DHCP responses to one portal.	*page 20-37*
dhcp-sniff-state	Records mobile unit DHCP state information	*page 20-38*
dot11-shared-key-auth	Enables support for 802.11 shared key authentication	*page 20-39*
end	Ends the current mode and moves to the EXEC mode	*page 20-40*
exit	Ends the current mode and moves to the previous mode	*page 20-41*
fix-broadcast-dhcp-rsp	Converts broadcast DHCP server responses to unicast responses	*page 20-42*
help	Displays the interactive help system	*page 20-43*
hotspot	Configures Hotspot configuration information.	*page 20-44*
ids	Sets intrusion detection configuration commands	*page 20-45*
load-balance	Sets the user load balance mode	*page 20-50*
mac-auth-local	Defines the local MAC authentication list	*page 20-51*
manual-wlan-mapping	Allows the manual mapping/un-mapping of WLANs to configured radios	*page 20-53*
mobile-unit	Configures mobile unit parameters	*page 20-54*
mobility	Configures mobility parameters	*page 20-55*
multicast-packet-limit	Sets a multicast packet limit (per second) for a VLAN	*page 20-56*
multicast-throttle-watermark	Configures watermarks for handling bursts of broadcast/multicast frames	*page 20-57*

Command	Description	Ref.
nas-id	Configures the NAS ID to be sent to the RADIUS server.	*page 20-58*
nas-port-id	Configures the NAS port to be sent to the RADIUS server.	*page 20-59*
no	Negates a command or sets its defaults	*page 20-60*
proxy-arp	Responds to ARP requests from the RON to a WLAN on behalf of MUs	*page 20-61*
qos-mapping	Defines the QoS mapping between wired and wireless domains	*page 20-62*
radio	Defines the radio's configuration	*page 20-64*
rate-limit	Sets the default rate limit (per user)	*page 20-78*
secure-wispe-default-secret	Configure default shared secret for secure wispe	*page 20-79*
self-heal	Sets the self healing configuration	*page 20-80*
sensor	Defines the *Wireless Intrusion Protection System* (WIPS) configuration	*page 20-82*
service	Invokes service commands to troubleshoot or debugs the `(config-wireless)` instance configuration	*page 20-84*
show	Displays running system information	*page 20-97*
smart-rf	Config Smart-RF Management Parameters	*page 20-100*
smart-scan-channels	Specify a list channels to motorola clients to perform smart-scan	*page 20-101*
wlan	Sets WLAN related parameters	*page 20-102*
wlan-bw-allocation	Allocates radio bandwidth (per WLAN)	*page 20-129*

20.1.1 aap

Wireless Configuration Commands

Defines the AAP configuration

Supported in the following platforms:

- RFS7000
- RFS6000



The number of AAP's supported differ from switch to switch.

- RFS7000 – Supports up to 256 AAP's
- RFS6000 – Supports up to 64 AAP's

Syntax

```
aap [aap-version|auto-upgrade|config-apply|fwupdate]
aap aap-version [aap5131|aap7131] <version-number>
aap auto-upgrade enable
aap config-aaply [def-delay|mesh-delay] <3-10000>
aap fwupdate [<index-num>|<MAC>|unadopted]
```

Parameters

aap-version [aap5131|aap7131] <version-number>	Enables version number • aap5131 • aap7131 • <version-number> – Configures minimum ap version required for adoption. A firm version string in the format X.X.X.X-XXXR
auto-upgrade enable	Enables automatic firmware upgrade of Adaptive AP on the switch

config-apply [def-delay|mesh-delay] <30-10000>	Applies AAP configuration settings • def-delay – Sets the default time to delay before applying AAP configuration • <30 -10000> – Set the delay time (in seconds) • mesh-delay – Defines the interval to delay before applying AAP configuration to Mesh APs • <3--10000> – Set the delay time (in seconds)
fwupdate [<index-num>|<MAC>| unadopted]	Manually upgrades the specified Advanced AP. The options are: • <index-num> – Updates the AAP based on its index number • <MAC> – Updates the AAP based on its MAC Address. An AAP can be updated based on either a single MAC address or a list of MAC addresses or a range of MAC addresses. Use the `show wireless ap` command to view the AP index • unadopted – Updates the unadopted AAPs

Usage Guidelines

Use **`{no} aap auto-upgrade enable`** to disable the auto-upgrade facility on the switch

Example

```
RFSwitch(config-wireless)#aap config-apply mesh-delay 300
RFSwitch(config-wireless)#
```

20.1.2 admission-control

Wireless Configuration Commands

Enable admission control for voice traffic across all radios

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
admission-control voice enable
```

Parameters

voice enable	Enables admission control for voice on all radios.

Usage Guidelines

Use **{no} admission-control voice enable** to disable Admission Control for voice or video on all radios.

Example

```
RFSwitch(config-wireless)#admission-control voice enable
RFSwitch(config-wireless)#
```

20.1.3 adopt-unconf-radio

Wireless Configuration Commands

Adopts a radio (even if not yet configured). Default templates are used for configuring the adopted radio

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
adopt-unconf-radio enable
```

Parameters

None

Usage Guidelines

Use the **{no} adopt-unconf-radio** command to switch off adopting unconfigured radios.

Example

```
RFSwitch(config-wireless)#adopt-unconf-radio enable
RFSwitch(config-wireless)#
```

20.1.4 adoption-pref-id

Wireless Configuration Commands

Preference identifier for the switch

All radios configured with this preference identifier are more likely to be adopted by this switch.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
adoption-pref-id <pref-id>
```

Parameters

<pref-id>	Set a preference ID with a numeric value in the range of 1-65535

Example

```
RFSwitch(config-wireless)#adoption-pref-id 500
RFSwitch(config-wireless)#
```

20.1.5 ap

Wireless Configuration Commands

Defines the name, location and other parameters of access ports

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap [<ap-index>|<ap-index-list>|<MAC>] [adoption-policy|
country-code|location|name|secure-mode|secure-mode-staging]

ap <ap-index> adoption-policy [allow|deny]
ap <ap-index> country-code <country-code>
ap <ap-index> location <location>
ap <ap-index> name <name>
ap <ap-index> secure-mode [enable|secret [0 <secret>|
                        2 <secret>|<secret>]
ap <ap-index> secure-mode-staging enable

ap <ap-index-list> adoption-policy [allow|deny]
ap <ap-index-list> country-code <country-code>
ap <ap-index-list> location <location>
ap <ap-index-list> name <name>
ap <ap-index-list> secure-mode [enable|secret [0 <secret>|
                        2 <secret>|<secret>]
ap <ap-index-list> secure-mode-staging enable

ap <MAC> adoption-policy [allow|deny]
ap <MAC> country-code <country-code>
ap <MAC> location <location>
ap <MAC> name <name>
ap <MAC> secure-mode [enable|secret [0 <secret>|
                        2 <secret>|<secret>]
ap <MAC> secure-mode-staging enable
```

Parameters

<ap-index> [adoption-policy| country-code|location| name|secure-code| secure-mode-stagging]	Sets a single AP index. Use the `show wireless ap` command to view the AP's index value. • adoption-policy [allow|deny]– Specifies adoption policy • allow – Allow adoption • deny – Deny adoption • country-code <country-code> – Defines the country of operation for the ap. Regulatory configurations such as channels will be configured automatically. • location <location> – Defines the location description of the AP • <location> – A string of upto 40 characters • name <name>– Sets the name of this AP • <name> – A string of upto 40 characters • secure-mode [enable|secret] – WISPe secure mode. Configures a shared secret to a set of APs (specified by LIST). The AP's MAC, shared secret will be saved in the running configuration file. If this command is not executed for an AP, default pre-shared secret will be assigned. • enable – Configure secure-mode to a set of APs (specified by LIST). The AP's MAC and mode will be saved in the running configuration. If secure-mode is enabled, the WISP-e for this AP is secured • secret [0 <secret>|2 <secret>|<secret>] – Secret is a string of up to 64 characters • 0 – Password is specified UNENCRYPTED • 2 – Password is specified encrypted with password-encryption secret • <secret> – If the secret <secret> is not specified then default secret will be used

	• secure-mode-staging enable – WISPe secure mode staging • enable – Configure secure-mode staging to a set of APs (specified by LIST). The AP's MAC, and staging mode will be saved in the running configuration. In this mode, switch will send configured shared secret in the clear in the Join response to the AP. • Use the `{no} secure-mode-staging enable` command to negate.
<ap-index-list> [adoption-policy|ccountry-code|location|name|secure-code|secure-mode-stagging]	A list (eg: 1,3,7) or range (eg: 3-7) of AP indices from the `show wireless ap` command
<MAC-address> [adoption-policy|country-code|location|name|secure-code|secure-mode-stagging]	Lists an AP's MAC address.

Usage Guidelines

Use `{no} ap <LIST> secure-mode secret` to reset a shared secret for a set of APs (specified by LIST) to the default shared secret. It is saved in the running configuration file.

Use `{no} ap <list> secure-mode enable` to disable secure-mode to a set of APs (specified by LIST). The AP's MAC, and mode will be saved in the running configuration.

Use `{no} ap <list> secure-mode-staging enable` to disable secure-mode staging to a set of APs (specified by LIST). The AP's MAC, and staging mode will be saved in the running configuration. In this mode, switch will not send at all configured shared secret in the Join response to the AP and AP will not get adopted by the switch.

Example

```
RFSwitch(config-wireless)#ap 00-15-70-14-FE-C4 location 5th
Floor SalesUnit
RFSwitch(config-wireless)#ap 1 location SJ NewPark
RFSwitch(config-wireless)#
```

20.1.6 ap-containment

Wireless Configuration Commands

Sets the rogue AP containment parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-containment [add <MAC>|enable|interval <interval>)
```

Parameters

add <MAC>	Adds an AP's MAC Address <MAC> into the rogue AP containment list.
enable	Enables the Rogue AP Containment feature.
interval <interval>	Sets the time <interval>, a value in the rage of 20-5000, between two Rogue AP containment processes. Time duration is in milliseconds.

Example

```
RFSwitch(config-wireless)#ap-containment enable
RFSwitch(config-wireless)#ap-containment interval 300
RFSwitch(config-wireless)#ap-containment add 00-15-70-37-fa-
be
RFSwitch(config-wireless)#
```



NOTE: The effective ap -containment interval for APs is 200ms which is channel dwell time. This remains same even if it configured to a lower value. For single-scan-APs, the smaller values of containment will be effective.

20.1.7 ap-detection

Wireless Configuration Commands

Configures access port detection parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-detection [approved|enable|mu-assisted-scan|timeout]
ap-detection approved add <list-index> [<MAC>|any]
ap-detection enable
ap-detection mu-assisted-scan [enable|refresh <refresh-
period>]
ap-detection timeout [approved|unapproved] <timeout>
```

Parameters

approved add <list-index> [<MAC>|any]	Sets the approved access port list • add <list-index> – Adds an entry to the approved access port list at the index <list-index>. • <MAC> – The a MAC address <MAC> in AA-BB-CC-DD-EE-FF format. • any– Assigns any MAC address.
enable	Allows access ports to look for APs
mu-assisted-scan [enable| refresh <refresh-period>]	Sets mobile unit assisted scanning configuration • enable – Enables mobile unit assisted scanning • refresh <refresh-period>> – Defines the period <refresh-period> (300 – 86400) (in seconds) used by all scan-capable mobile units are polled to scan for neighboring access ports.

ap-detection timeout [approved|unapproved] <timeout>	Sets the amount of time (in seconds) an AP remains in the list after it is no longer seen • approved <timeout> – The timeout <timeout> in seconds for approved APs. • unapproved <timeout> – The timeout <timeout> in seconds for unapproved APs

Example

```
RFSwitch(config-wireless)#ap-detection enable
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ap-detection approved add 150 any
any
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ap-detection mu-assisted-scan
enable
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ap-detection mu-assisted-scan
refresh 520
RFSwitch(config-wireless)#
```

20.1.8 ap-image

Wireless Configuration Commands

Defines the path to upload the new image over an AP

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-image [ap100|ap300-ids-sensor|ap300-wisp|ap300-wispe|
ap4131|ap5131|ap7131|revert-ap4131] <file-path>
```

Parameters

[ap100| ap300-ids-sensor| ap300-wisp| ap300-wispe| ap4131|ap5131|ap7131| revert-ap4131] <file-path>	The interface to upload new AP image. The following APs are supported: • ap100 – AP image for AP100 • ap300-ids-sensor – IDS Sensor firmware for AP300 • ap300-wisp – WISP image for AP300 • ap300-wispe – WISPe image for AP300 • ap4131 – AP image for AP4131 • ap5131 – Adaptive AP image for AP5131 • ap7131 – Adaptive AP image for AP7131 • revert-ap4131 – AP image for revert-AP4131 • <file-path> – Path of the new AP-Image

Example

```
RFSwitch (config-wireless)#ap-image ap5131 flash:/
aap_10B.bin
RFSwitch (config-wireless)#
```

20.1.9 ap-ip

Wireless Configuration Commands

Modifies the static IP address for an access port

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-ip [<AP-list/MAC>|default-ap]

ap-ip <AP-list/MAC> [static-ip|switch-ip]
ap-ip <AP-list/MAC> static-ip <IP/Mask> <gateway-IP>
ap-ip <AP-list/MAC> switch-ip [add <IP>|
delete [<IP>|<IP-index>]|<IP>|set-default]
ap-ip default-ap [add <IP address>|delete [<IP|<IP-index>]|
<IP address>)|set-default]
```

Parameters

ap-ip <AP-list/MAC> [static-ip|switch-ip]	Use show wireless ap to view an AP's index or MAC address. Select the AP's index / MAC Address to modify its static IP address. • static-ip <IP/Mask> <gateway-IP> – Sets the static IP address, netmask and gateway address of the AP • <IP/Mask> – Defines the static IP address and mask • <gateway-IP>– Sets the gateway IP address • switch-ip [add <IP>| delete [<IP>|<IP-index>]|<IP>|set-default] – Defines the static switch IP address • add <IP> – Adds a static switch IP address <IP> • delete [<IP-index>|<IP>] – Deletes a static switch IP address • <IP-index> – A single switch IP address in the range 1-12. • <IP> – A single IP address • set-default – Default switch IP address

default-ap switch-ip [add <IP-list>| delete [<IP-index>|<IP>]| set-default]	Sets the default static switch IP address • switch-ip – Static switch IP address • add – Adds a static switch IP address • delete[<IP-index>|<IP>] – Deletes a static switch IP address • <IP-index> – A single switch IP address • <IP> – A single IP address • set-default – Sets a default switch IP address

Example

```
RFSwitch(config-wireless)#ap-ip 1 static-ip 192.168.10.25/24
192.168.10.1
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ap-ip 1 switch-ip add
192.168.10.25 10.10.1.4
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ap-ip default-ap switch-ip set-
default
RFSwitch(config-wireless)#
```

20.1.10 ap-standby-attempts-threshold

Wireless Configuration Commands

Sets the number of attempts after which the standby switch starts adopting APs.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-standby-attempts-threshold <attempts>
```

Parameters

<attempts>	Sets the number of attempts to <attempts> in the range 5–200.

Example

```
RFSwitch(config-wireless)#ap-standby-attempts-threshold 100
RFSwitch(config-wireless)#
```

20.1.11 ap-timeout

Wireless Configuration Commands

Changes the default inactivity timeout for access ports

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-timeout <index> <timeout>
```

Parameters

<index> <timeout>	• <index> – Access-ports identified by a single index or by a list of indices. Use show wireless ap to view the AP's index or MAC address • <timeout> – Sets the new inactivity timeout (in seconds) to a value between 40 and 180.

Example

```
RFSwitch(config-wireless)#ap-timeout 1 40
RFSwitch(config-wireless)#
```

20.1.12 ap-udp-port

Wireless Configuration Commands

Configures the UDP port for layer 3 adoption of APs

You also need to configure the DHCP server providing the APs the same parameter.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ap-udp-port <port>
```

Parameters

<port>	Sets the port number for layer 3 adoption of APs. <port> is a value in the range 1-65535.

Example

```
RFSwitch(config-wireless)#ap-udp-port 20
RFSwitch(config-wireless)#
```

20.1.13 auto-select-channels

Wireless Configuration Commands

Specifies a list of channels that will be used when *automatic channel scan* (ACS) and *dynamic frequency selection* (DFS)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
auto-select-channels [11a|11bg] [<channel-list>|
  add <channel-list>|remove <channel-list>]
```

Parameters

[11a|11bg] [<channel-list>| add <channel-list>| remove <channel-list>]	A comma separated list of 802.11a or 802.11bg channels • <channel-list> – a list of comma separated channels • add <channel-list> – adds <channel-list> channels to existing list • remove <channel-list>– remove <channel-list> channels from existing list

Example

```
RFSwitch(config-wireless)#auto-select-channels 11a 1,3,5
RFSwitch(config-wireless)#
```

20.1.14 broadcast-tx-speed

Wireless Configuration Commands

Configure the rate at which broadcast and multicast traffic is transmitted between the switch and mobile unit

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
broadcast-tx-speed [range|throughput]
```

Parameters

range	Uses a lowest basic rate, but provides the maximum range
throughput	Uses a highest basic rate, but provides the maximum throughput (default)

Example

```
RFSwitch(config-wireless)#broadcast-tx-speed range
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#broadcast-tx-speed throughput
RFSwitch(config-wireless)#
```

20.1.15 client

Wireless Configuration Commands

Use this command to configure a wireless client

This command creates an exclude-list or include list. Creating a list moves the user to a new mode `config-wireless-client-list`.

Refer section *config-wireless-client-list Commands on page 20-26* for `(config-wireless-client-list)` command summary.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
client [exclude-list|include-list] <list-name>
```

Parameters

exclude-list <list-name>	Sets the wireless client exclude list configuration. A MU NAC check is conducted, except for those in the exclude list. Devices in the exclude list will not have a NAC check performed.
include-list <list-name>	Defines the wireless client include list configuration. No MU NAC check is conducted, except for those in the include list. Devices in the include-list will have NAC checks.
<list-name>	Name of the list to be created.

Example

```
RFSwitch(config-wireless)#client exclude-list JustMe
RFSwitch(config-wireless-client-list)#
```

20.1.15.1 Configuring a Client

Refer to the configurations below to:

- Create an exclude list.

```
RFSwitch(config-wireless)#client exclude-list protected-hosts
RFSwitch(config-wireless-client-list)#
```

- Add a host entry into the exclude list.

```
RFSwitch(config-wireless-client-list)# station printers
00:00:AA:DD:EE:11/00:00:FF:DD:EE:11

RFSwitch(config-wireless-client-list)# station testing-host1
00:11:AA:03:1B:FE
```

- Associate the exclude list to a WLAN.

```
RFSwitch(config-wireless-client-list)# wlan 1
```

- Configure RADIUS server parameters.

```
RFSwitch(config-wireless)# wlan 1 nac-server primary 192.168.0.1
RFSwitch(config-wireless)# wlan 1 nac-server primary secret 0
testing
RFSwitch(config-wireless)# wlan 1 nac-server secondary 192.168.1.1
RFSwitch(config-wireless)# wlan 1 nac-server secondary secret 0
testing123
```

- Enable NAC for a WLAN.

```
RFSwitch(config-wireless)# wlan 1 nac-mode do-nac-except-exclude-
list
```

- Undo a configuration.

```
RFSwitch(config-wireless)# client exclude-list protected-hosts
RFSwitch(config-wireless-client-client)# no station testing-host1
RFSwitch(config-wireless)# no client exclude-list protected-hosts
RFSwitch(config-wireless)# no wlan 1 nac-server primary
RFSwitch(config-wireless)# no wlan 1 nac-server primary secret
RFSwitch(config-wireless)# no wlan 1 nac-server secondary
RFSwitch(config-wireless)# no wlan 1 nac-server secondary
radius-key
RFSwitch(config-wireless)# no wlan 1 nac exclude-list
protected-hosts
```

20.1.15.2 config-wireless-client-list Commands

Use `(config-wireless)# client` to enter the `(config-wireless-client-list)` instance. Use this instance, to create an exclude list or include list.

This table summarizes `config-wireless-client-list` commands:

Command	Description
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system
no	Negates a command or sets its defaults
service	Provides a means of troubleshooting and debugging
show	Displays running system information
station	Defines a MU's MAC configuration
wlan	Sets Wireless LAN related parameters

station

config-wireless-client-list Commands

Adds a specified MAC entry into the client's exclude or include list

Syntax

```
config-wireless-client-list station <host-name> [<MAC>|
<MAC/Mask>]
```

Parameters

<host-name> [<MAC>|<MAC/Mask>]	Defines an index for this host entry in the client list. The host station name <host-name> must be of size 1-21 characters. • <MAC> –Sets the MU mac address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format. • <MAC/Mask> – Sets the MU MAC address and mask in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format.

Example

```
RFSwitch(config-wireless-client-list)#station ExcludeList1
AA:BB:CC:DD:EE:FF
RFSwitch(config-wireless-client-list)#
```

wlan

config-wireless-client-list Commands

Adds a client exclude list name into/from the WLAN

Syntax

```
wlan [<index>|<index-list>]
```

Parameters

wlan [<index>| <index-list>]	• <index> – Sets a single WLAN index in the range 1-256 • <index-list> – A list (1,3,7) or range (3-7) of WLAN indices

Example

```
RFSwitch(config-wireless-client-list)#wlan 1
RFSwitch(config-wireless-client-list)#
```

20.1.16 clrscr

Wireless Configuration Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-wireless)#clrscr
RFSwitch(config-wireless)#
```

20.1.17 cluster-master-support

Wireless Configuration Commands

Sets the parameters for cluster master support

This is required for cluster level functions.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
cluster-master-support enable
```

Parameters

enable	Enables the cluster master support. This is required for cluster level functions.

Usage Guidelines

Use the **{no} cluster-master-support enable** command to disable this feature. By default, it is disabled.

Example

```
RFSwitch(config-wireless)#cluster-master-support enable
RFSwitch(config-wireless)#
```

20.1.18 convert-ap

Wireless Configuration Commands

Changes the mode of operation of an AP to either sensor or standalone

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: The number of APs supported by `convert-ap` command differs for each switch.

- RFS7000 supports <1-256> APs
- RFS6000 supports <1-64> APs

Syntax

```
convert-ap <ap-index> [default|sensor|standalone]

convert-ap <ap-index> [default|standalone]
convert-ap <ap-index> sensor {static-ip <IP/Mask>
  {<gateway-IP>}}
```

Parameters

<ap-index> [default|sensor| standalone]	Sets the indices of the APs to be converted. • <ap-index> – The index of the AP to be converted. This index can be found from the 'show wireless ap' command. • default – Does not force conversion. Lets the AP negotiate its normal mode of operation with the switch. • sensor {static-ip <IP/Mask> {<gateway-IP>}}– Converts an AP300 to operate as an IPS (*Intrusion Prevention System*) sensor. • static-ip <IP/Mask> – Optional. Sensor must use specific static IP address. • <IP/Mask> – Sensor IP address and network mask. • <gateway-IP> – Optional. Specify gateway IP address for sensors **NOTE:** The switch will not be able to adopt this AP again until it is converted back to a AP300 using the `sensor <1-256> revert-to-ap` command • standalone – Converts a thin AP-4131 back to a stand-alone AP. **NOTE:** The switch will not be able to adopt this AP again until the AP is converted back to a thin-AP using the AP's configuration interface.

Example

```
RFSwitch(config-wireless)#convert-ap 1 default
```

20.1.18.1 Converting an AP to Sensor

To convert an AP300 to a sensor:

1. Use `sensor` command to setup the sensor.

   ```
   RFSwitch(config-wireless)#sensor default-config ?
   ip-mode         configure the IP address mode of the sensors
   wips-server-ip  specify IP addresses of the WIPS server
   ```

   Select either `ip-mode` or `wips-server-ip` as the sensor parameter.

2. Specify the VLAN over which the sensors are available. This will help the switch detect them.

   ```
   RFSwitch(config-wireless)#sensor vlan 10
   ```

3. Use `convert-ap` command to convert the selected AP into a sensor directly from the switch.

   ```
   RFSwitch(config-wireless)#convert-ap 1 sensor
   ```



NOTE: To convert multiple APs' to Sensor, do it one by one and do config modifications.

20.1.19 country-code

Wireless Configuration Commands

Sets the country of operation

All existing radio configurations will be erased

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
country-code <country-code>
```

Parameters

<country-code>	Configures the switch to operate in a defined country. <country-code> is the 2 letter ISO-3166 country code.

Usage Guidelines

Use the `show wireless country code` command to view the list of supported countries

Example

```
RFSwitch(config-wireless)#country-code ?
WORD  the 2 letter ISO-3166 country code ("show wireless
country-code-list" to see list of supported countries)

RFSwitch(config-wireless)#country-code US
RFSwitch(config-wireless)#
```

20.1.20 debug

Wireless Configuration Commands

Debugging functions for the Cellcontroller (wireless)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`debug cc [access-port|all|alt|ap-containment|ap-detect|capwap|cluster|config|dot11|eap|ids|kerberos|l3-mob|loc-ap|loc-mu|media|mobile-unit|radio|radius|self-heal|smart|snmp|system|wips|wisp|wlan] {debug|err|info|warn}`

Parameters

access-port	Sets the parameters for the access-port logs
all	Sets the parameters for all the modules
alt	Sets the parameters for the address lookup logs
ap-containment	Sets the parameters for the ap-containment logs
ap-detect	Sets the parameters for the Rogue AP detection logs
capwap	Sets the parameters for the CAPWAP logs
cluster	Sets the parameters for the cluster related logs
config	Sets the parameters for the configuration change logs
dot11	Sets the parameters for the datapath logs
eap	Sets the parameters for the 802.11x eap logs
ids	Sets the parameters for the intrusion detection logs
kerberos	Sets the parameters for the kerberos logs
l3-mob	Sets the parameters for the Layer-3 mobility logs
loc-ap	Sets the parameters for the AP locationing logs

loc-mu	Sets the parameters for the MU locationing logs
media	Sets the parameters for the encapsulation media logs
mobile-unit	Sets the parameters for the mobile-unit logs
radio	Sets the parameters for the radio logs
radius	Sets the parameters for the radius client logs
self-heal	Sets the parameters for the self healing logs
smart	Sets the parameters for the smart-rf logs
snmp	Sets the parameters for the snmp logs
system	Sets the parameters for the system call logs
wips	Sets the parameters for the WIPS sensor logs
wisp	Sets the parameters for the WISP logs
wlan	Sets the parameters for the WLan logs

For all the above parameters, the following optional values are set:

debug	all the messages are logged
err	only error and higher severity messages are logged
info	only information and higher severity messages are logged
warn	only warning and higher severity messages are logged

Example

```
RFSwitch(config-wireless)#debug cc ?
access-port     access-port logs
all             all modules
alt             address lookup logs
ap-containment  rogue AP containment logs
ap-detect       rogue AP detection logs
capwap          capwap logs
cluster         cluster related logs
```

```
config          configuration change logs
dot11           datapath logs
eap             802.1x/eap logs
ids             intrusion detection logs
kerberos        kerberos logs
l3-mob          Layer3 mobility logs
loc-ap          loc-ap logs
loc-mu          loc-mu logs
media           encapsulation media logs
mobile-unit     mobile-unit logs
radio           radio logs
radius          radius client logs
self-heal       Self Healing logs
smart           smart-rf logs
snmp            SNMP logs
system          system call logs
wips            WIPS sensor logs
wisp            WISP logs
wlan            wlan logs

RFSwitch(config-wireless)#

RFSwitch(config-wireless)#debug cc system warn
RFSwitch(config-wireless)#debug cc l3-mob err
RFSwitch(config-wireless)#debug cc config debug
RFSwitch(config-wireless)#debug cc kerberos info
RFSwitch(config-wireless)#
```

20.1.21 dhcp-one-portal-forward

Wireless Configuration Commands

Enables the option to forward DHCP responses to one portal when the destination mobile-unit is known from the response content

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
dhcp-one-portal-forward enable
```

Parameters

enable	Enables the option to forward DHCP responses to one portal when the destination mobile-unit is known from the response content.

Usage Guidelines

Use the **`{no} dhcp-one-portal-forward enable`** command to disable forwarding DHCP responses.

Syntax

```
RFSwitch(config-wireless)#dhcp-one-portal-forward enable
RFSwitch(config-wireless)#
```

20.1.22 dhcp-sniff-state

Wireless Configuration Commands

Records mobile unit DHCP state information

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
dhcp-sniff-state enable
```

Parameters

enable	Allows support for recording DHCP state information for mobile units

Use the **`{no} dhcp-sniff-state enable`** command to disable recording mobile unit DHCP state information.

Example

```
RFSwitch(config-wireless)#dhcp-sniff-state enable
RFSwitch(config-wireless)#
```

20.1.23 dot11-shared-key-auth

Wireless Configuration Commands

Enables support for 802.11 shared key authentication



NOTE: Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accommodate wireless stations unable to carry out Open-System authentication.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
dot11-shared-key-auth enable
```

Parameters

enable	Enables support for shared key authentication

Usage Guidelines

Use the **{no} dot11-shared-key-auth enable** command to disable support for 802.11 shared key authentication.

Example

```
RFSwitch(config-wireless)#dot11-shared-key-auth enable
RFSwitch(config-wireless)#
```

20.1.24 end

Wireless Configuration Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-wireless)#end
RFSwitch#
```

20.1.25 exit

Wireless Configuration Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-wireless)#exit
RFSwitch(config)#
```

20.1.26 fix-broadcast-dhcp-rsp

Wireless Configuration Commands

Converts broadcast DHCP server responses to unicast

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
fix-broadcast-dhcp-rsp enable
```

Parameters

enable	Enables support for converting broadcast DHCP server responses to unicast

Usage Guidelines

Use the **`{no} fix-broadcast-dhcp-rsp enable`** command to disable converting broadcast DHCP server responses to unicast.

Example

```
RFSwitch(config-wireless)#fix-broadcast-dhcp-rsp enable
RFSwitch(config-wireless)#
```

20.1.27 help

Wireless Configuration Commands

Displays the system's interactive help (in HTML format)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-wireless)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
RFSwitch(config-wireless)#
```

20.1.28 hotspot

Wireless Configuration Commands

Configures the WLAN hotspot configuration

This overrides or adds to the existing hotspot configuration on the WLAN.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
hotspot query <query-index> <query-field> [mu-ip|ssid|
  switch-ip|switch-name|user-string]
```

Parameters

<query-index>	The index of this query in the query list. Can be in the range of 1 and 10.
<query-field> [mu-ip|ssid|switch-ip|switch-name|user-string]	The name of the field in the URL whose value is substitute with the parameters • mu-ip – The MU's IP address • ssid – The WLAN's SSID • switch-ip – The switch's router ip-address for the external hotspot server • switch-name – The switch's name on the network • user-string – Specifies that the value of the query is a user string.

Example

```
RFSwitch(config-wireless)# hotspot query 1 user-name user-
string
RFSwitch(config-wireless)# hotspot query 2 from mu-ip
RFSwitch(config-wireless)#
```

20.1.29 ids

Wireless Configuration Commands

Defines the *Wireless Intrusion Detection System* (WIDS) configuration

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
ids [anomaly-detection|detect-window|ex-ops]

ids anomaly-detection [all|bad-essid-frame|
  beacon-broadcast-essid|deauth-broadcast-smac|
  detect-adhoc-networks|invalid-8021x-frame|
  invalid-frame-length|invalid-frame-type|
  invalid-sequence-number|multicast-source|
  non-changing-wep-iv|null-destination|
  same-source-destination|tkip-countermeasures|
  unencrypted-traffic|weak-wep-iv]
  [enable|filter-ageout <ageout>]
ids anomaly-detection bad-essid-frame [<1-10> <info>|enable|
  filter-ageout <ageout>]

ids detect-window <duration>

ids ex-ops [80211-replay-fails|all|association-requests|
  authentication-fails|crypto-replay-fails|
  decryption-fails|disassociations|eap-naks|eap-starts|
  probe-requests|unassoc-frames] [filter-ageout <0-86400>|
  threshold [mu|radio|switch] <0-65535>]
```

Parameters

anomaly-detection [all|bad-essid-frame| beacon-broadcast-essid| deauth-broadcast-smac| detect-adhoc-networks| invalid-8021x-frame| invalid-frame-length| invalid-frame-type| invalid-sequence-number| multicast-source| non-chaining-wep-iv| null-destination| same-source-destination| tkip-countermeasures| unencrypted-traffic| weak-wep-iv] [enable|filter-ageout]	Configures parameters related to the detection of anomalous frames on the RF network. The parameters are: • all – Enables all types of anomalous frames • bad-essid-frame{<1-10> <info>}– Enables an AP detector to configure up to 10 known bad ESSIDs • <1-10> – Configure list of known bad ESSIDs • <info> – A string of upto 32 characters • beacon-broadcast-essid – Enables an AP detector to find beacons with broadcast ESSIDs • deauth-broadcast-smac – Enables monitoring and filtering of broadcast deauthentication messages from a source. • detect-adhoc-networks – Detects adhoc networks. • invalid-8021x-frame – Detects invalid 802.1x frames • invalid-frame-length – Detects frames with an invalid length • invalid-frame-type – Detects frames with an invalid type • invalid-sequence-number – Detects frames with invalid sequence numbers • multicast-source – Broadcast or multicast source • non-changing-wep-iv – Detects frames with a non changing WEP IV • null-destination – Detects addresses with all zeros • same-source-destination – Identical source and destination addresses • tkip-countermeasures – Filters mobile units causing TKIIP countermeasures • unencrypted-traffic – Detects unencrypted-traffic • weak-wep-iv – Uses weak WEP sequence numbers

	For all the above options, the following values are set • enable – Enables monitoring and filtering • filter-ageout <ageout>– Sets the number of seconds mobile units are filtered out in the range 0-86400.
detect-window <duration>	Sets the number of seconds <duration> information is collected before analysis (all thresholds are a function of this window size). Value in the range 5-300.

ex-ops [80211-replay-fails|all| association-requests| authentication-fails| crypto-replay-fails| decryption-fails| disassociations| eap-naks|eap-starts| probe-requests| unassoc-frames] [filter-ageout <0-86400>| threshold [mu|radio| switch] <0-65535>]	Sets values related to the detection of excessive operations on the RF network • 80211-replay-fails – 802.11 replay check failure • all – Changes for all types of excessive operations • association-requests – 802.11 authentication and association requests • authentication-fails – Failure to authenticate with servers (RADIUS/Kerberos) • crypto-replay-fails – TKIP/CCMP IV replay check failure • decryption-fails – Decryption failures • disassociations – Disassociation and deauthentication frames • eap-naks – Excessive EAP-NAKs • eap-starts – EAP (802.1x) start frames • probe-requests – Probe request frames • unassoc-frames – Frames from unassociated stations For all the above options, the following values are set • filter-ageout <0-86400> – Sets the number of seconds mobile units will be filtered out • threshold [mu|radio|switch] <0-65535> – Sets the threshold allowed in the detection window • mu – Uses the threshold for monitoring on a per mobile unit basis • radio – Uses the threshold for monitoring on a per radio basis • switch – Uses the threshold for monitoring at the switch level

Example

```
RFSwitch(config-wireless)#ids anomaly-detection tkip-
countermeasures enable
RFSwitch(config-wireless)#


RFSwitch(config-wireless)#ids detect-window 250
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#ids ex-ops 80211-replay-fails
filter-ageout 5200
RFSwitch(config-wireless)#
```

20.1.30 load-balance

Wireless Configuration Commands

Configures the user load balance mode

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
load-balance [by-count|by-throughput]
```

Parameters

by-count	In load balance by user count, the load on the radio is measured by the number of MUs associated. The desired balance is to have equal number of MUs on the radios in the group. By default, the load balance is configured for *by-count* when the switch boots up with factory default configuration.
by-throughput	In load balance by radio throughput (threshold 1 Mbps) the load on the radio is measured by the current average throughput rate. The desired balance is to have similar wireless traffic on the radios in the group.

Example

```
RFSwitch(config-wireless)#load-balance by-throughput
RFSwitch(config-wireless)#
```

20.1.31 mac-auth-local

Wireless Configuration Commands

Configures the local MAC authentication list

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mac-auth-local <1-1000> [allow|deny|rate-limit]

mac-auth-local <1-1000> [allow|deny] <starting-MAC>
  <ending-MAC> [<list>|not-mapped] {<radio-desc>|
  zone [<1-48>|default|unknown]}

mac-auth-local <1-1000> rate-limit
[wired-to-wireless|wireless-to-wired] <100-1000000>
```

Parameters

<1-1000>	Sets the mac-auth-local entry index to a value between 1 and 1000.
allow	Allows mobile units that match this rule to associate.
deny	Denies association to mobile units that match this rule.
rate-limit	Sets the rate limit value for this ACL entry.
<starting-MAC>	Starting MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF format.
<ending-MAC>	Ending MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF format.
<list>	Configures the local MAC authentication list.Sets the list (1,3,7) or range (3-7) of WLAN indices.
not-mapped	An unmapped row in the ACL.
<radio-desc>	Optional radio description substring.

zone [<1-48>|default| unknown]	Optional GeoFencing location information for devices matching this ACL information. • <1-48> – Administrator defined-id. • default – The user has been located within the site in the default zone. • unknown – If the users location is currently unknown or out of bounds of the site.
rate-limit [wired-to-wireless| wireless-to-wired] <100-1000000>	Set the rate limit for ACL • wired-to-wireless – Sets rate for down link direction from network to. wireless client. • wireless-to-wired – Sets the rate for up link direction from wireless client to network. • <100-1000000> – The rate in kbps.

Example

```
RFSwitch(config-wireless)#mac-auth-local 1 allow
01:02:03:04:05:06 01:02:03:04:05:07 not-mapped
RFSwitch(config-wireless)#mac-auth-local 2 deny
01-20-30-40-50-60 01-20-30-40-50-70 not-mapped
RFSwitch(config-wireless)#mac-auth-local 1 allow
01:02:03:04:05:06 01:02:03:04:05:07 not-mapped zone 1
```

20.1.32 manual-wlan-mapping

Wireless Configuration Commands

Manually maps WLANs configured on a radio

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
manual-wlan-mapping enable
```

Parameters

enable	Enables support for manual WLAN mapping.

Usage Guidelines

Use the **{no} manual-wlan-mapping enable** command to disable manual mapping of WLANs configured on a radio.

Example

```
RFSwitch(config-wireless)#manual-wlan-mapping enable
RFSwitch(config-wireless)#
```

20.1.33 mobile-unit

Wireless Configuration Commands

Configures mobile unit related parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mobile-unit [association-history|probe-history]

mobile-unit association-history [enable|clear]
mobile-unit probe-history [enable|add <1-200> <MAC>]
```

Parameters

association-history [enable|clear]	Enables a mobile unit's association history. • enable – Enables a mobile unit's association history. • clear – Clears the association history for all mobile units.
probe-history [enable|add <1-200> <MAC>	Mobile unit probe logging configuration commands. • enable – Enables a mobile unit's probe logging feature. • add <1-200> <MAC>– Adds a mobile unit to probe history logging. • <1-200> – Select an index value between 1 and 200 to add probe logging MAC. • <MAC> – Sets the MAC address of the mobile used for probe history logging

Example

```
RFSwitch(config-wireless)#mobile-unit probe-history enable
RFSwitch(config-wireless)#mobile-unit association-history
enable
RFSwitch(config-wireless)#mobile-unit probe-history add 20
AA-BB-CC-DD-EE-FF
RFSwitch(config-wireless)#
```

20.1.34 mobility

Wireless Configuration Commands

Sets mobility parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mobility [enable|local-address|max-roam-period|peer]

mobility enable
mobility local-address <IP>
mobility max-roam-period <1-15>
mobililty peer <IP>
```

Parameters

enable	Enables mobility globally
local-address <ip>	Sets the local address for mobility • <IP> – IP address in A.B.C.D format
max-roam-period <1-300>	Sets the Max Roam Period for a mobile unit (in seconds) to a value in the range of 1 and 300.
peer <ip>	Adds a peer to this mobility region • <IP> – IP address of the Peer in A.B.C.D format

Example

```
RFSwitch(config-wireless)#mobility enable
RFSwitch(config-wireless)#mobility local-address 12.12.12.1
RFSwitch(config-wireless)#mobility max-roam-period 10
RFSwitch(config-wireless)#mobility peer 157.208.235.108
RFSwitch(config-wireless)#
```

20.1.35 multicast-packet-limit

Wireless Configuration Commands

Sets a multicast packet limit, per second, for a VLAN. This limits the broadcast/multicast packets per VLAN. The default value is 32 broadcast/multicast packets per second. Setting the limit to 0 disables this control.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
multicast-packet-limit <0-128> [<vlan-id>|<vlan-id-range>]
```

Parameters

<0-128>	Sets the multicast packet limit per second.
<vlan-id>	Defines the single VLAN ID in the range 1-4094 the new limit applies to.
<vlan-id-range>	Defines a list of VLAN IDs in the format 1,3,7 or range 3-7 of VLAN IDs

Example

```
RFSwitch(config-wireless)#multicast-packet-limit 120 50
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#multicast-packet-limit 120 1,10,25
RFSwitch(config-wireless)#
```

20.1.36 multicast-throttle-watermark

Wireless Configuration Commands

Configures watermarks for supporting bursts of broadcast/multicast frames

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
multicast-throttle-watermarks low <0-100> high <0-100>
```

Parameters

low <0-100>	Sets the low water-mark. If the percentage of free packets in the system is lower than this threshold, the incoming frame is dropped.
high <0-100>	Sets the high water-mark. If the percentage of free packets in the system is between the low water-mark and this value, the packet is subjected to a random-early-drop. If free packets are greater than this value, the packet is processed.

Example

```
RFSwitch(config-wireless)#multicast-throttle-watermarks low
10 high 20
RFSwitch(config-wireless)#
```

20.1.37 nas-id

Wireless Configuration Commands

Configures the NAS ID to be sent to the RADIUS server

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
nas-id <nas-id>
```

To override nas-id on a per WLAN basis:

```
wlan <1-4098> nas-id <nas-id>
```

Parameters

<nas-id>	A character string to be used as the NAS ID. Can be up to 256 characters long.

Example

```
RFSwitch(config-wireless)#nas-id WIRELESSWELL
RFSwitch(config-wireless)#
RFSwitch(config-wireless)#wlan 1 nas-id WIRELESSWELL1
```

20.1.38 nas-port-id

Wireless Configuration Commands

Configures the NAS port ID that must be sent to the RADIUS server

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
nas-port-id <port-id>
```

Parameters

<port-id>	The port ID to be sent to the RADIUS server.

Example

```
RFSwitch(config-wireless)#nas-port-id portWIRELESSWELL
RFSwitch(config-wireless)#
```

20.1.39 no

Wireless Configuration Commands

Negates a command or sets its defaults. All the parameters mentioned in the syntax can be negated using the **no** command.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [aap|admission-control|adoption-pref-id|
adopt-unconf-radio|ap|ap-containment|ap-detection|ap-image|
ap-ip|ap-standby-attempts-threshold|ap-timeout|ap-udp-port|
auto-select-channel|broadcast-tx-speed|client|
cluster-master-support|country-code|debug|
dhcp-one-portal-forward|dhcp-sniff-state|
dot11-shared-key-auth|fix-broadcast-dhcp-rsp|hotspot|ids|
mac-auth-local|manual-wlan-mapping|mobile-unit|mobility|
multicast-packet-limit|multicast-throttle-watermarks|nas-id|
nas-port-id|proxy-arp|qos-mapping|radio|rate-limit|
secure-wispe-default-secret|self-heal|sensor|service|
smart-scan-channels|wlan|wlan-bw-allocation]
```

Parameters

Refer to the individual commands for the parameters negated using the **no** command.

Example

```
RFSwitch(config-wireless)#no mobility enable
RFSwitch(config-wireless)#
```

20.1.40 proxy-arp

Wireless Configuration Commands

Responds to ARP requests from the RON to the WLAN on behalf of mobile units

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
proxy-arp enable
```

Parameters

enable	Enables the support for proxy arp

Usage Guidelines

Use the **no proxy-arp** enable command to disable.

Example

```
RFSwitch(config-wireless)#proxy-arp enable
RFSwitch(config-wireless)#
```

20.1.41 qos-mapping

Wireless Configuration Commands

Configures QoS mappings between the wired and wireless domains

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
qos-mapping [wired-to-wireless|wireless-to-wired]

qos-mapping wired-to-wireless [dot1p <0-7>|dscp <0-63>]
[<0-7>|tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7]

qos-mapping wireless-to-wired
[tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7] dot1p <0-7>
```

Parameters

wired-to-wireless [dot1p <0-7>|dscp <0-63>] [<0-7>|tid0|tid1|tid2|tid3|tid4|tid5|tid6|tid7]	Mappings used while switching wired traffic over the air . • dot1p <0-7> – Configures the mapping of 802.1p tags to access categories. You can specify more than one 802.1p tags with in the range 0 and 7. • dscp <0-63> – Configures the mapping of DSCP values to access categories. You can specify more than one DSCP values in the range 0-63. • tid0, tid3– best effort category traffic • tid1, tid2 – background category traffic • tid4, tid5 – video traffic category traffic • tid6, tid7 – voice traffic category traffic

wireless-to-wired [tid0|tid1|tid2|tid3| tid4|tid5|tid6|tid7] dot1p <0-7>	Mappings used while switching wireless traffic to the wired side. • tid0, tid3– best effort category traffic • tid1, tid2 – background category traffic • tid4, tid5 – video traffic category traffic • tid6, tid7 – voice traffic category traffic • dot1p <0-7> – Configures the mapping of 802.1p tags to access categories. You can specify more than one 802.1p tags with in the range 0 and 7.

Example

```
RFSwitch(config-wireless)#qos-mapping wireless-to-wired
background dot1p 5
RFSwitch(config-wireless)#
```

20.1.42 radio

Wireless Configuration Commands

Sets radio related parameters

Supported in the following platforms:

- RFS7000
- RFS6000



The radios `group-id` range differs from switch to switch.

- RFS7000 – Supports a range between 0-255
- RFS6000 – Supports a range between 0-64

Syntax

```
radio [<1-4096>|<radio-list>|add|all-11a|all-11an|all-11b|
  all-11bg|all-11bgn|antenna-mode|configure-8021X|
  default-11a|default-11an|default-11b|default-11bg|
  default-11bgn|dns-name]

radio [<1-4096>|<radio-list>|all-11a|all-11an|all-llb|
  all-11bg|all-11bgn|default-11a|default-11an|default-11b|
  default-11bg||default-11bgn] [admission-control|
  adoption-policy|adoption-pref-id|ampdu|antenna-mode|
  base-bridge|beacon-interval|bridge-fwd-delay <4-30>|
  bridge-hello <1-10>|bridge-max-ageout <4-3600>|
  bridge-msg-age <6-40>|bridge-priority <0-65535>|bss|
  channel-power|client-bridge|copy-config-from|description|
  detector|dtim-period|enforce-spec-mgmt|
  enhanced-beacon-table|enhanced-probe-table|
  group-id [<0-48>|<0-255>|<0-64>]|location-led|
  location-message|mac|max-mobile-units|
  moto-simple-voice enable|mu-power <0-20>|nas-id|
  nas-port-id|on-channel-scan|radio-number|reset|reset-ap|
  rf-function|rf-mode|rss|rts-threshold|run-acs|
  self-heal-offset|short-gi|short-preamble|speed|timeout|
  tunnel|wmm]

radio <1-4096> admission control voice [max-mu <1-256>|
  max-perc <1-100>|max-roamed-mus <0-256>|
  res-roam-perc <0-100>]

radio <1-4096> adoption-policy [allow|deny]

radio <1-4096> adoption-pref-id <0-65535>
```

```
radio <1-4096> ampdu [min-spacing|rx-limit|tx-enable|
  tx-limit]
radio <1-4096> ampdu min-spacing [.25|.5|0|1|2|4|8]
radio <1-4096> ampdu rx-limit [16383|32767|65535|8191]
radio <1-4096> ampdu tx-enable
radio <1-4096> ampdu tx-limit <0-65535>

radio <1-4096> antenna-mode [diversity|mimo|primary|
  secondary]

radio <1-4096> bss [<1-4>|add-wlans|auto]<wlan-list>
radio <1-4096> base-bridge [enable|max-clients <1-12>]
radio <1-4096> beacon-interval <50-200>
radio <1-4096> bridge-fwd-delay <4-30>
radio <1-4096> bridge-hello <1-10>
radio <1-4096> bridge-max-ageout <4-3600>
radio <1-4096> bridge-msg-age <6-40>
radio <1-4096> bridge-priority <0-65535>

radio <1-4096> channel-power [indoor|outdoor] [<1-200>|acs|
  random] <4-20> [20Mhz|40Mhz]
radio <1-4096> client-bridge [enable|mesh-timeout <2-200>|
  ssid <SSID>]
radio <1-4096> client-bridge [bb-radio|bridge-select-mode]
radio <1-4096> client-bridge bb-radio <1-16> <radio-MAC>
radio <1-4096> client-bridge bridge-select-mode
  [auto|manual]
radio <1-4096> copy-config-from [<1-4096>|default-11a|
  default-11b|default-11bg]

radio <1-4096> description <description>
radio <1-4096> dtim-period <1-50> bss <1-4>
radio <1-4096> detector

radio <1-4096> enforce-spec-mgmt enable
radio <1-4096> enhanced-beacon-table
radio <1-4096> enhanced-probe-table

radio <1-4096> group-id <1-256>

radio <1-4096> location-led [start-flashing|stop-flashing]
radio <1-4096> location-message <message>

radio <1-4096> mac <MAC>
```

```
radio <1-4096> max-mobile-units <units>
radio <1-4096> mu-power <0-20>
radio <1-4096> moto-simple-voice enable

radio <1-4096> nas-id <nas-id>
radio <1-4096> nas-port-id <nas-port-id>

radio <1-4096> on-channel-scan

radio <1-4096> radio-number <0-2>
radio <1-4096> reset
radio <1-4096> reset-ap
radio <1-4096> rf-function wips
radio <1-4096> rf-mode [a|an|b|bg|bgn|custom|g|n]
radio <1-4096> rss enable
radio <1-4096> rts-threshold <0-2346>
radio <1-4096> run-acs

radio <1-4096> self-heal-offset <0-30>
radio <1-4096> short-gi enable
radio <1-4096> short-preamble

radio <1-4096> speed [1|11|12|18|2|24|36|48|54|5p5|6|9|
  basic1|basic11|basic11a|basic11an|basic11b1|basic11b2|
  basic11bg|basic11bgn|basic11g|basic11gn|basic11n|
  basic12|basic18|basic2|basic24|basic36|basic48|basic54|
  basic5p5|basic6|basic9|default|range|throughput]

radio <1-4096> timeout <40-180>
radio <1-4096> tunnel tx-rate-class <1-4>

radio <1-4096> wmm [background|best-effort|video|voice]
  [aifsn <1-15>|burst <0-65535>|cw <0-15>]

radio [all-lla|default-11a] [admission-control|
  adoption-policy|adoption-pref-id|antenna-mode|base-bridge|
  beacon-interval|bridge-fwd-delay|bridge-hello|
  bridge-max-ageout|bridge-msg-age|bridge-priority|bss|
  channel-power|client-bridge|detector|dtim-period|
  enforce-spec-mgmt|enhanced-beacon-table|
  enhanced-probe-table|location-led|
  location-message|max-mobile-units|moto-simple-voice|
  mu-power|on-channel-scan|reset|reset-ap|rf-function|
  rf-mode|rss|rts-threshold|run-acs|self-heal-offset|speed|
  wmm|tunnel]
```

radio [all-llan|default-11an] [adoption-policy|ampdu|
antenna-mode|bss|channel-power|rf-mode|speed|tunnel|
short-gi]

radio [all-11b|default-11b] [adoption-policy|
antenna-mode|base-bridge|beacon-interval|bridge-fwd-delay|
bridge-hello|bridge-max-ageout|bridge-msg-age|
bridge-priority|bss|channel-power|client-bridge|detector|
dtim-period|enhanced-beacon-table|enhanced-probe-table|
location-message|max-mobile-units|mu-power|
on-channel-scan|reset|reset-ap|rf-function|rf-mode|rss|
rts-threshold|run-acs|self-heal-offset|speed|tunnel|
short-preamble]

radio [all-11bg|default-11bg] [admission-control|
adoption-policy|adoption-pref-idantenna-mode|base-bridge|
beacon-interval|bridge-fwd-delay|bridge-hello|
bridge-max-ageout|bridge-msg-age|bridge-priority|bss|
channel-power|client-bridge|detector|dtim-period|
enhanced-beacon-table|enhanced-probe-table|location-led
location-message|max-mobile-units|moto-simple-voice|
mu-power|on-channel-scan|reset|reset-ap|rf-function|
rf-mode|rss|rts-threshold|run-acs|self-heal-offset|
speed|tunnel|short-preamble|wmm]

radio [all-llbgn|default-11bgn] [adoption-policy|ampdu|
antenna-mode|bss|channel-power|rf-mode|speed|tunnel|
short-gi]

radio **add** <1-4096> <MAC> [11a|11an|11b|11bg|11bgn]
{[aap5131|aap5181|ap300|aap7131|aap7181|ap100|ap4131]}

radio antenna-mode [diversity|mimo|primary|secondary]

radio configure-8021X <username> <password> *{<MAC>}*

radio dns-name <dns-name> *{<MAC>}*

Parameters

<1-4096>	Defines a single radio index.
<radio-list>	Creates a list (1,3,7) or range (3-7) of radio indices.

add <1-4096> <MAC> [11a|11an|11b|11bg|11bgn] *{[aap5131|aap5181|ap300|aap7131|aap7181|ap100|ap4131]}*	Adds the specified radio to the radio list at index specified for the value in the range 1-4096. • [11a|11an|11b|11bg|11bgn] – The radio type • [aap5131|aap5181|ap300|aap7131|aap7181|ap100|ap4131] – Optional. The radio model. The options available will depend on the radio type selected.
all-11a	All 11a radios currently in configuration
all-11an	All 11an radios currently in configuration
all-11b	All 11b radios currently in configuration
all-11bg	All 11bg radios currently in configuration
all-11bgn	All 11bgn radios currently in configuration
antenna-mode [diversity|mimo|primary|secondary]	Antenna diversity mode. Select diversity from: • diversity – Use full diversity (both antennas) • mimo – use MIMO • primary – Use primary antenna only • secondary – Use secondary antenna only
configure-8021X	Configures the 802.1X username and password on adopted access ports
default-11a	Adopts the default 11a configuration template
default-11an	Adopts the default 11an configuration template
default-11b	Adopts the default 11b configuration template
default-11bg	Adopts the default 11bg configuration template
default-11bgn	Adopts the default 11bgn configuration template

The following is the list of parameters for the **`radio <1-4096>, radio [all-11a|all-11an|all-11b|all-11bg|all-11bgn|default-11a||default-11an|default-11b|default-11bg|default-11bgn]`** commands.

admission-control voice [max-mus <0-256>| max-perc <0-100>| max-roamed-mus <0-256>| res-roam-perc <0-100>]	Sets the admission control parameters for voice. The following options are configured: • max-mus <0-256> – Configure the maximum number of MUs to be admitted. • max-perc <0-100> – Configure the maximum percentage of air time allotted to voice traffic. • max-roamed-mus <0-256> – Configure the maximum number of roamed MUs to be admitted. • res-roam-perc <0-100> –Configure the maximum percentage of air time exclusively allotted to MUs that have roamed. This value is calculated relative to the max-perc value.
adoption-pref-id <0-65535>	Employs a preference identifier for this radio port. The radio port is more likely to be adopted by a wireless switch that is a preferred switch.
adoption-policy [allow|deny]	Specifies adoption policy. Select from : • allow – Allows adoption • deny – Denies adoption
ampdu [min-spacing [.25|.5|0|1|2|4|8]| rx-limit [16383|32767| 65535|8191]| tx-limit <0-65535>| tx-enable *{min-spacing [.25|.5|0|1|2|4|8]| rx-limit [16383|32767| 65535|8191]| tx-limit <0-65535>}*	Specifies the settings for the MAC Protocol frames. The following properties are configured: • min-spacing [.25|.5|0|1|2|4|8] – The spacing between MPDUs received in microseconds. • rx-limit [8191|16283|32767|65535] – The receive buffer limit in bytes. • tx-limit <0-65535> – The transmit buffer limit in bytes. • tx-enable {min-spacing [.25|.5|0|1|2|4|8]|rx-limit [16383|32767|65535|8191]|tx-limit <0-65535>} – Optional parameters for enabling transmitting A-MPDUs.

antenna-mode [diversity|mimo|primary|secondary]	Defines the antenna diversity mode. Select from the following options: • diversity–Full diversity (both antennas) • mimo – MIMO • primary–Primary antenna only • secondary–Secondary antenna only **Note:** Before executing this command, ensure the radio is present and is a AP300 model.
base-bridge [enable| max-clients <1-12>]	Sets base bridge values • enable – Allows the given radio to act as a base bridge and accept connections from client bridges. • max-clients <1-12> – Configures a base-bridge. Enter maximum client bridges allowed.
beacon-interval <50-200>	Sets the beacon interval (in K-uSec)
bridge-fwd-delay <4-30>	Sets the STP bridge forward delay (in seconds) • <4-30> - Time in seconds
bridge-hello <1-10>	Sets the STP bridge hello (in seconds) • <1-10> - Time in seconds
bridge-max-ageout <4-3600>	Sets the STP bridge maximum ageout (in seconds) • <4-3600> - Time in seconds
bridge-msg-age <6-40>	Sets the STP bridge message age (in seconds) • <6-40> - Time in seconds
bridge-priority <0-65535>	Sets the STP bridge priority (in seconds) • <0-65535> - Priority value

bss [<1-4>|add-wlans| auto] <wlans>	Maps WLANs to radio BSSIDs • <1-4>– Sets the BSS where WLANs are mapped • add-wlans <wlans> – Adds new WLANs to existing radios. The other WLANs on the radios are left as is. • auto <wlans> – Sets the automatic assignment of a BSS. The user selects WLANs, and the system assigns them to a BSS automatically. • <wlans> – Defines a list (1,3,7) or range (3-7) of WLAN indices. When a BSS is also specified, the first WLAN is used as the primary WLAN. When the auto option is used, the system automatically assigns the first four WLANs as primaries on their respective BSSIDs.
channel-power [indoor|outdoor] [<1-200>|acs|random]	Sets the location, channel and transmit power level • indoor [<1-200>|acs|random]– Defines an indoor location • <1-200> <4-20> {[lower|upper]} – Defines the channel number • <4-20> – Power in dBm • lower – Lower channel width mode • upper – Upper channel width mode • outdoor [<1-200>|acs|random]– Defines an outdoor location • <1-200> – Sets the channel number • <4-20> – Sets the power in dBm • acs <4-20> {[20 MHz | 40 Mhz]} – Enables ACS (*auto channel selection*). A radio will scan for the least congested channel at startup or switch reconfiguration. • random <4-20> {[20 MHz | 40 Mhz]} – Random channel selection

client-bridge [bb-radio| bridge-selectmode| enable| mesh-timeout <2-200>| ssid <SSID>]	Defines client bridge settings. • bb-radio <1-16> <MAC>– add the preferred base bridge details. • <1-16> – Enables the capability • MAC – MAC address in AA-BB-CC-DD-EE-FF format • bride-select-mode [auto|manual]– Base bridge selection mode • auto – Automatically select base bridge • manual – Manually select base bridge • enable – Enables client-bridge functionality on radio • mesh-timeout [0|1|<2-200>] – Sets the client bridge link timeout. • 0 – Disable uplink detection • 1 – Uplink detect - shutdown when all mesh-backhaul links are down • <2-200> – Timeout in seconds. • ssid <SSID> – Defines the ESSID of the WLAN
copy-config-from [<1-4096>|default-11a| default-11b| default-11bg|]	Copies the configuration from a previously configured radio. • <1-4096> – Defines a single radio index • default-11a – Uses the default 11a configuration template. • default-11b – Uses the default 11b configuration template. • default-11bg – Uses the default 11bg configuration template.
description <description>	Defines a description for this radio. <description> is a 20 character string.
detector	Dedicates this radio as a detector. No mobile units can associate to a detector.

dtim-period<1-50> *{bss <1-4>}*	Set the DTIM period (number of beacons between successive DTIMs). • <1-50> – Sets the DTIM period • bss <1-4>– Optional BSS index
enforce-spec-mgmt enable	Enforces spectrum management checks on specified radios. Only mobile units that advertise spectrum management capabilities will be allowed to associate on this radio.
enhanced-beacon-table	Enables the enhanced beacon table for AP locationing.
enhanced-probe-table	Enables the enhanced probe table for MU locationing.
group-id <1-256>	Specifies the radio groups to balance user load. • For RFS7000, <0-255> – Radio group identifier used for an access-port, 0 disables the grouping. • For RFS6000, <0-64> – Radio group identifier used for an access-port, 0 disables the grouping.
location-led [start-flashing| stop-flashing]	Changes the mode of operation of the LEDs on an AP. • start-flashing – Requests parent-ap of specified radio to begin flashing its LEDs to help locate it. • stop-flashing – Requests parent-ap of specified radio to revert its LEDs to normal mode of operation.
location-message <message>	Specifies a message sent to all mobile units that associate with these radios. This message <message> should not exceed 80 characters.
mac <MAC>	Changes the parent (access-port) MAC address of the radio.
max-mobile-units <1-256>	Maximum number of mobile units allowed to associate.
mu-power <0-20>	Power adjustment level for mobile units associated with this access-port. MUs that support this element will reduce their transmit power by the specified value. • <0-20> – Power adjustment level in dBm.

nas-id <ID>	Configures a NAS ID for this radio. <ID> can be up to 256 characters long.
nas-port-id <ID>	Configures a NAS port id for this radio. <ID> can be up to 256 characters long.
on-channel-scan	Enables rogue scanning on this radio.
radio-number <0-2>	Enter the radio number only if there are two similar radios on the AP. Enter 0 (zero) or omit when there is no ambiguity.
reset	Resets a radio (this will only reset the specified radio, not the complete access port).
reset-ap	Resets the parent AP (this will reset all radios on that access port).
rf-function wips	Selects the rf-function for the selected radio. • wips – Selects WIPS sensor mode.
rf-mode [a|an|b|bg|bgn|custom|g|n]	Selects the radio speed based on the radio mode selected.
rss enable	*Remote Site Survivability* (RSS) enables the delivery of secure uninterrupted wireless service in remote locations in the event of a device failure.
rts-threshold <0-2347>	Defines the RTS threshold in bytes.
run-acs	Runs an auto-channel-selection on a radio. The radio should already have been configured for ACS support.
self-heal-offset <0-30>	Configures the self-healing offset (measured in dBm), for regulatory compliance. **Note:** The offset is based off the regulatory maximum power for the specified channel ("show wireless regulatory" displays the max power allowed).
short-gi enable	Enables the Short GI value for both the 20 MHz and the 40 MHz channels for the 11n radio.

short-preamble	Enables support for the short preamble. **NOTE:** This disables support for long preamble. Mobiles that only support long preamble will not be able to associate.
speed [1|11|12|18|2|24|36|48|54|5p5|6|9|basic1|basic11|basic11a|basic11an|basic11b1|basic11b2|basic11bg|basic11bgn|basic11g|basic11gn|basic11n|basic12|basic18|basic2|basic24|basic36|basic48|basic54|basic5p5|basic6|basic9|range|throughput|default]	Configures the basic and supported data rates/speed • 1 1-Mbps • 11 11-Mbps • 12 12-Mbps • 18 18-Mbps • 2 2-Mbps • 24 24-Mbps • 36 36-Mbps • 48 48-Mbps • 54 54-Mbps • 5p5 5.5-Mbps • 6 6-Mbps • 9 9-Mbps • basic1 basic 1-Mbps • basic11 basic 11-Mbps • basic11a rate set (6,12,24 Mbps) • basic11an rate set (6,12,24, MCS 0-7) • basic11b1 rate set (1 and 2 Mbps) • basic11b2 rate set (1,2,5.5,11 Mbps) • basic11bg rate set (1,2,5.5,11,6,12,24 Mbps) • basic11bgn rate set (1,2,5.5,11,6,12,24, MCS 0-7) • basic11g rate set (6,12,24 Mbps) • basic11gn rate set (6,12,24, MCS 0-7) • basic11n rate set (MCS 0-7) • basic12 basic 12-Mbps • basic18 basic 18-Mbps • basic2 basic 2-Mbps • basic24 basic 24-Mbps • basic36 basic 36-Mbps • basic48 basic 48-Mbps

	• basic54 basic 54-Mbps • basic5p5 basic 5.5-Mbps • basic6 basic 6-Mbps • basic9 basic 9-Mbps • default {mcs <msc-range>} – Factory default rates based on radio-type. • throughput {mcs <msc-range>} – All rates basic (only 802.11g clients are allowed on 802.11bg radios). • range {mcs <msc-range>} – all rates enabled, the lowest one set to basic • mcs – Configure the mcs rates / speed • MCS – A list or range (eg: 0-5, 10,15) of MCS rates (0 to 15)
timeout <40-180>	The time out value in seconds for the selected radio.
tunnel tx-rate-class <1-4>	The tunnel transmit rate class for the radio. Select a value from 1 to 4.

wmm [background| best-effort|video|voice] [aifsn<1-15>|burst <0-65535>| cw<0-15>] wmm [video|voice] acm [enable|max-mus <1-64>]	Sets *802.11e/Wireless Multi Media* (WMM) parameters (supported only on AP300). • background – Prioritizes Background category traffic. • best-effort– Prioritizes Best Effort category traffic. • video – Prioritizes Video category traffic. • voice – Prioritizes Voice category traffic. • acm [enable|max-mus <1-64>] – Admission control parameters. Use `enable` to allow admission control.Enabling ACM on video enables ACM on the Voice access category. Use `max-mus` to specify the number of mobile units that are allowed access on the specified categories. • aifsn <1-15> – *Arbitration Inter Frame Spacing Number* (AIFSN) defines the wait time (in milliSeconds) between data frames. Derived using AIFSN and the slot-time. • burst <0-65535> – Transmit-opportunity. Sets an interval when a particular WMM STA has the right to initiate transmissions onto the wireless medium. • cw <0-15> – *Contention Window* (cw) parameters. Wireless stations pick a number between 0 and the minimum contention window to wait before re-trying transmissions. Stations then double their wait time on a collision, until it reaches the maximum contention window.

Example

```
RFSwitch(config-wireless)#radio 250 bss auto 3-5
RFSwitch(config-wireless)#
```

20.1.43 rate-limit

Wireless Configuration Commands

Sets the default rate limit per user in kbps, and applies to all enabled WLANs

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rate-limit [wired-to-wireless|wireless-to-wired] <0-100000>
```

Parameters

wired-to-wireless <100-100000>	Down link direction from network to wireless client • <100-100000> – rate in the range of <100-100000> kbps
wireless-to-wired <100-100000>	Up link direction from wireless client to network • <100-100000> – rate in the range of <100-100000> kbps

Usage Guidelines

Use **{no} rate-limit [wired-to-wireless|wireless-to-wired]** to remove the rate limit applied to the group

Example

```
RFSwitch(config-wireless)#rate-limit wired-to-wireless 1000
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#rate-limit wireless-to-wired 20000
RFSwitch(config-wireless)#
```

20.1.44 secure-wispe-default-secret

Wireless Configuration Commands

Configures the default shared secret for secure WISPE

If a new shared secret is not configured for an AP or a list of APs, then a default shared secret will be assigned. The value of default shared secret is the string "default".

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
secure-wispe-default-secret [<secret-key>|0 <secret-key>|
  2 <secret-key>]
```

Parameters

[<secret-key>| 0 <secret-key>| 2 <secret-key>]	Enter a secret key. The string length must not exceed 64 characters. • 0 <secret-key> – Password is specified unencrypted. • 2 <secret-key>– Password is specified encrypted with password-encryption secret. • <secret-key> – 8 to 64 characters.

Example

```
RFSwitch(config-wireless)#secure-wispe-default-secret
0x1d8e4fc780be92537109
RFSwitch(config-wireless)#
```

20.1.45 self-heal

Wireless Configuration Commands

Configures self healing values

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
self-heal [interference-avoidance|neighbor-recovery]

self-heal interference-avoidance [enable|hold-time
<30-65535>|retries <0.0-15.0>]

self-heal neighbor-recovery [action|enable|neighbors|
run-neighbor-detect]
self-heal neighbor-recovery action [both|none|open-rates|
raise-power] radio [<1-4096>|<radio-list>]
self-heal neighbor-recovery neighbors <1-4096> [<1-4096>|
<radio-list>]
self-heal neighbor-recovery run-neighbor-detect
```

Parameters

interference-avoidance	Interference avoidance configuration.
enable	Enables/disables interference avoidance.
hold-time <30-65535>	The number of seconds to disable interference avoidance after a detection. This prevents a radio from changing channels continuously. Set the hold-time between 30-65535 seconds.
retries <0.0-15.0>	Defines the average number retries (0-15) causing a radio to re-run auto channel selection.
neighbor-recovery	Invokes neighbor recovery configuration commands.

action [both|none| open-rates|raise-power] radio [<1-4096>| <radio-list>]	Defines the radio's self healing action when neighbors are detected as down. • both – Raises the power to max and open all rates. • none – No action taken. • open-rates – Opens all rates. • raise-power – Raises the power to maximum. • radio [<1-4096>|<radio-list>] – Modifies the action for specified radio(s). • <1-4096> – Sets a single radio index. • <radio-list> – Defines a list (1,3,7) or range (3-7) of radio indices.
enable	Monitors access ports and attempts to increase coverage on a detected failure.
neighbors <1-4096> [<1-4096>|<radio-index>]	Adds a radio as a neighbor. • <1-4096> – Sets a single radio index. • <radio-list> – Defines a list (1,3,7) or range (3-7) of radio indices.
run-neighbor-detect	Disassociates all mobile units, clears current neighbors and runs neighbor detection again.

Example

```
RFSwitch(config-wireless)#self-heal interference-avoidance
enable
RFSwitch(config-wireless)#self-heal interference-avoidance
hold-time 600
RFSwitch(config-wireless)#self-heal neighbor-recovery enable
Note: reducing the configured transmit power of radios will
ensure that there is room to increase power when a neighbor
fails
RFSwitch(config-wireless)#self-heal neighbor-recovery
neighbors 1 1
RFSwitch(config-wireless)#
```

20.1.46 sensor

Wireless Configuration Commands

Configures *Wireless Intrusion Protection System* (WIPS) parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
sensor [<1-48>|default-config|ping-interval|vlan]
sensor <1-48> [default-config|request-config|revert-to-ap]

sensor default-config [gateway-ip|ip-mode|wips-server-ip]
sensor default-config gateway-ip <IP>
sensor default-config ip-mode [dhcp|static <IP/Mask>]
sensor default-config wips-server-ip [primary|secondary]
  <IP>
sensor ping-interval <2-60>
sensor vlan <1-4094> {<1-4094>}
```

Parameters

<1-48> [defaultconfig| requestconfig| revert-to-ap]	Select a sensor to reset/revert the AP to its original state. Use the **`show wireless sensor`** command to view the sensor index. • default-config – Restores the internal configuration of the sensor to default values. This sends the configuration to the sensor. • request-config – Polls the sensor for its latest configuration. • revert-to-ap – Reverts an IDS sensor back to an access port that can service mobile-units.

default-config [gateway-ip|ip-mode| wips-server-ip]	Invokes the default configuration sent to sensors when configured. • gateway-ip <IP> – Configure the gateway IP address for sensors to <IP>. • ip-mode [dhcp|static <IP/Mask>] – Configures the IP address of the sensors. • dhcp – Sensors use DHCP to obtain an IP address. • static <IP/Mask> – Sensors use the specific static IP address. • <IP/Mask> – Sets the sensor IP address and network mask. • wips-server-ip [primary|secondary] <IP> – Specifies the IP addresses of the WIPS server. • primary <IP> – Specifies the primary IP address of the WIPS server. • secondary <IP> – Specifies the secondary IP address of the WIPS server.
ping-interval <2-60>	Sets the ping interval (in seconds) between successive pings to sensors on the network.
vlan <1-4094>	Configures VLANs where sensors are discovered. • <1-4094> – Vlan IDs

Example

```
RFSwitch(config-wireless)#sensor vlan 268 500
RFSwitch(config-wireless)#
```

20.1.47 service

Wireless Configuration Commands

Invokes service commands to troubleshoot or debug `(config-wireless)` instance configurations

For more information, see *Chapter 2, Section 2.1.5 service* on *page 2-7*.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service [clear|show|smart-rf|wireless]

service clear wireless mobile-unit association-statistics

service show [cli|smart-rf|wireless]
service show cli

service show smart-rf [debug-config|sensitivity]
service show smart-rf debug-config
service show smart-rf sensitivity [mu|pattern|rates]
service show smart-rf sensitivity mu {[<0-8192>|<MAC>]}
service show smart-rf sensitivity pattern [pattern-11a|
  pattern-11b|pattern-11bg|pattern-2-mbps]
service show smart-rf sensitivity rates <rate-flag>

service show wireless [ap-history|buffer-counters|
  enhanced-beacon-table|enhanced-probe-table|group|
  group-stats|legacy-load-balance|mu-cache-buckets|
  mu-cache-entry|mvlan|radio|radio-cache-entry|
  radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|
  vlan-cache-entry|waiting]
service show wireless [buffer-counters|group-stats|
  legacy-load-balance|mu-cache-buckets|radio-hash-buckets|
  snmp-trap-throttle|vlan-cache-buckets]

service show wireless ap-history {<MAC>}
service show wireless enhanced-beacon-table [config|report]
service show wireless enhanced-probe-table [config|report]
service show wireless group <1-256>
service show wireless mu-cache-entry {[<1-8192>|<MAC>]}
service show wireless mvlan <1-256>
```

```
service show wireless radio {[<1-4094>|description|mapping]}
service show wireless radio-cache-entry {<MAC>}
service show wireless vlan-cache-entry {[<1-8192>|<MAC>]}
service show wireless waiting {<0-99> {<0-99>}}

service smart-rf [clear-history|load-from-file|replay|
  rescue|restore|save-to-file|simulate]
service smart-rf [clear-history|load-from-file|save-to-file]
service smart-rf replay enable
service smart-rf rescue [<MAC>|<1-4094>|<index-list>]
service smart-rf restore [<MAC>|<1-4094>|<index-list>]
service smart-rf simulate [coverage-hole|interference]
service smart-rf simulate coverage-hole <1-4096>
  <experienced-range> [<transmit-rate>|pattern-11a|
  pattern-11b|pattern-11bgn|pattern-2-mbps]
service smart-rf simulate interference [<MAC>|<1-4094>|
  <index-list>]

service wireless [ap-history|clear-ap-log|custom-cli|dot11i|
  dump-core|enhanced-beacon-table|enhanced-probe-table|
  free-packet-watermark|idle-radio-send-multicast|
  legacy-load-balance|map-radios|radio-misc-cfg|
  rate-scale|request-ap-log|save-ap-log|snmp-trap-throttle|
  sync-radio-entries|vlan-cache]
service wireless ap-history [clear|enable]
service wireless clear-ap-log {<ap-index>}
service wireless custom-cli [sh-wi-mobile-unit|sh-wi-radio]
service wireless custom-cli sh-wi-mobile-unit [ap-locn|
  ap-name|channel|dot11-type|ip|last-heard|mac|radio-bss|
  radio-desc|radio-id|ssid|state|vlan|wlan-desc|wlan-id|
  username]
service wireless custom-cli sh-wi-radio [adopt-info|
  ap-locn|ap-mac|ap-name|bss|channel|dot11-type|num-mu|
  power|radio-desc|radio-id|state]

service wireless dot11i enforce pmkid-validation

service wireless enhanced-beacon-table [channel-set|enable|
  erase-report|max-ap|scan-interval|scan-time]
service wireless enhanced-beacon-table [enable|erase-report]
service wireless enhanced-beacon-table channel-set
  [a|an|bg|bgn] <1-200>
service wireless enhanced-beacon-table max-ap <0-512>
service wireless enhanced-beacon-table scan-interval <10-60>
service wireless enhanced-beacon-table scan-time <100-1000>
```

```
service wireless enhanced-probe-table [enable|erase-report|
  max-mu|preferred|window-time]
service wireless enhanced-probe-table [enable|erase-report]
service wireless enhanced-probe-table max-mu <0-512>
service wireless enhanced-probe-table preferred <MAC>
service wireless enhanced-probe-table window-time <10-60>

service wireless free-packet-watermark <0-100>
service wireless idle-radio-send-multicast enable
service wireless map-radios <1-127>
service wireless radio-misc-cfg <hex-mask>
service wireless request-ap-log <ap-index>
service wireless snmp-trap-throttle <1-20>
service wireless vlan-cache enable
```

Parameters

clear wireless mobile-unit association-statistics	Clears statistics for wireless mobile unit associations and dis-associations.

show [cli|smart-rf|wireless]	Displays the current running system information for this mode. • cli – Shows the CLI commands available in this mode. • smart-rf [debug-config|sensitivity] – Displays smart-rf management commands. • debug-config – Displays smart-rf debug configuration information • sensitivity [mu|pattern|rates] – Displays the smart-rf sensitivity table. • mu {[<0-8192>|<MAC>]} – Displays smart-rf sensitivity information for a selected MU. • <0-8192> – Optional. MU index. • <MAC> – Optional. MU MAC address. • pattern [pattern-11a|pattern-11b|pattern-11bg|pattern-2-mbps] – Displays smart-rf common MU patterns. • pattern-11a – 11a MUs • pattern-11b – 11b MUs • pattern-11bg – 11bg MUs • pattern-2-mbps – 2-Mbps units • rates <rate-flag> – Displays rates. <rate-flag> is in hexadecimal format. • wireless [ap-history|buffer-counters|enhanced-beacon-table|enhanced-probe-table|group|group-stats|legacy-load-balance|mu-cache-buckets|mu-cache-entry|mvlan radio|radio-cache-entry|radio-hash-buckets|snmp-trap-throttle|vlan-cache-buckets|vlan-cache-entry|waiting] – Displays wireless parameters. • ap-history {<MAC>} – Displays access port history for all MACs. Provide the optional <MAC> parameter to view ap-history for a AP with that MAC address. • buffer-counters – Displays allocations for the different buffers.

	• enhanced-beacon-table [config|report] – Displays Enhanced Beacon Table information. • config – Displays Enhanced Beacon Table configuration information. • report – Displays Enhanced Beacon Table reports. • enhanced-probe-table [config|report] – Displays Enhanced Probe Table information. • config – Displays Enhanced Probe Table configuration information. • report – Displays Enhanced Probe Table reports • group <1-256> – Displays information on a radio group. • <1-256> – The radio group index to display information for. • group-stats – Displays radio group statistics. • legacy-load-balance – Displays legacy load balance algorithm compatibility mode. • mu-cache-buckets – Displays wireless mobile units cache buckets. • mu-cache-entry [<1-8192>|<MAC>] – Displays MU Cache information, dumps the whole MU Cache table if no parameters is given. • <1-8192> – An index in the MU Cache table. • <MAC> – MAC address of mu-cache entry to show. • mvlan <1-256> – Displays multi VLAN debug statistics. • <1-256> – A single wlan index. • radio [<1-4096>|description|mapping] – Displays radio serviceability parameters. • <1-4096> – A single radio index. • description – Description and location co-ordinates of radios. • mapping – Radio-to-CPU Mapping.

	• radio-cache-entry {<MAC>} – Displays Radio Cache information. Dumps the whole table if no parameter is given. • <MAC> – MAC address of radio-cache entry to show. • radio-hash-buckets – Displays Wireless Radio Hash Buckets. • snmp-trap-throttle – Displays statistics and parameters related to SNMP Trap Throttling. • vlan-cache-buckets – Displays wireless VLAN Cache Buckets. • vlan-cache-entry [<1-8192>|<MAC>] – Displays MU VLAN Cache information. Dumps whole table if no parameter is given. • <1-8192> – An index in the MU VLAN Cache table. • <MAC> – MAC address of VLAN cache entry to show. • waiting <0-99> – Displays waiting table contents. • <0-99> – Index in the waiting table.
smart-rf [clear-history| load-from-file|replay| rescue|restore| save-to-file|simulate]	Configures smart-rf parameters. • clear-history – Clears assignment history. • load-from-file – Loads smart-rf configuration from the file *smart.bin*. • replay enable – Enables replay mode for smart-rf • rescue [<MAC>|<1-4094>|<index-list>] – Forces radio rescue operation. • <MAC> – MAC address of a single radio. • <1-4094> – Radio index. • <index-list> – List of radio indices.

	• restore [<MAC>|<1-4094>|<index-list>] – Removes radio rescue operation on a given radio. • <MAC> – MAC address of a single radio. • <1-4094> – Radio index. • <index-list> – List of radio indices. • save-to-file – Saves smart-rf records to the file *smart.bin*. • simulate [coverage-hole|interference] – Simulates radio events for smart-rf. • coverage-hole <1-4096> <experienced-range> [<transmit-rate>|pattern-11a|pattern-11b|pattern-11bgn| pattern-2-mbps] – Simulates a coverage-hole radio event on the selected radio index. • <1-4096> – The radio index to simulate on. • <experienced-range> – The experienced range in Mbps. • <transmit-rate> – The provide simulated MU's allowed transmit rates in hexadecimal format. • pattern-11a – 11a units • pattern-11b – 11b units • pattern-11bg – 11bg units • pattern-2-mbps – 2 Mbps units • interference [<MAC>|<1-4094>|<index-list>] – Simulates an interference on a radio. • <MAC> – MAC address of a single radio. • <1-4094> – Radio index. • <index-list> – List of radio indices.

wireless [ap-history| clear-ap-log|custom-cli| dot11i|dump-core| enhanced-beacon-table| enhanced-probe-table| free-packet-watermark| idle-radio-send-multicast| legacy-load-balance|map-radios| radio-misc-cfg| rate-scale| request-ap-log| save-ap-log| snmp-trap-throttle| sync-radio-entries| vlan-cache]	Configures wireless parameters. • ap-history [clear|enable] – Configures access port history. • clear – Clears all history of all APs. • enable – Enables tracking of AP history. • custom-cli [sh-wi-mobile-unit|sh-wi-radio] – Customize the output of some summary cli commands in wireless. • sh-wi-mobile-unit [ap-locn|ap-name|channel| dot11-type|ip|last-heard|mac|radio-bss| radio-desc|radio-id|ssid|state|vlan|wlan-desc| wlan-id|username] – Customize the output of the "**`show wireless mobile-unit`**' command. • ap-locn – The location of the AP where the mobile-unit is associated. • ap-name – The name of the AP where the mobile-unit is associated. • channel – The channel of the radio where the mobile-unit is associated. • dot11-type – The dot11 radio type of the mobile-unit. • ip – The IP address of the mobile-unit. • last-heard – The time when a packet was last received from the mobile-unit. • mac – MAC address of mobile-unit. • radio-bss – The BSSID of the radio where the mobile-unit is associated. • radio-desc – Description of radio where the mobile-unit is associated. • radio-id – The radio index to which the mobile-unit is associated. • ssid – The SSID of the mobile-units wlan. • state – The current state of the mobile-unit.

	• username – The Radius username of the user connected through this device (shown only if applicable and available). • vlan – The VLAN-ID assigned to the mobile-unit. • wlan-desc – The WLAN description the mobile-unit is using. • wlan-id – The WLAN index the mobile-unit is using. • sh-wi-radio [adopt-info|ap-locn|ap-mac| ap-name|bss|channel|dot11-type|num-mu|power| radio-desc|radio-id|state] – Customize the output of the "**`show wireless radio`**" command. • adopt-info – The adoption information about the radio. • ap-locn – The location of the AP to which this radio belongs. • ap-mac – The MAC address of AP to which the radio belongs. • ap-name – The name of the AP to which this radio belongs. • bss – The BSSID of the radio. • channel –The configured and current channel of the radio. • dot11-type – The dot11 type (11a/11g etc) of the radio. • num-mu – The number of mobile devices associated with this radio. • power – The configured and current transmit power of the radio. • pref-id – The adoption preference ID of the radio. • radio-desc – The description of radio. • radio-id – The radio index in configuration. • state – The current operational state of the radio.

	• dot11i – modify dot11i service parameters. • dump-core – Creates a core file of the *ccsrvr* process. • enhanced-beacon-table [channel-set|enable|erase-report|max-ap|scan-interval|scan-time] – Enhanced beacon table for AP locationing. • channel-set [a|an|b|bg|bgn] <1-200> – Adds channels to the different radio types. Channel types are a, an, b, bg, bgn. The channel number must be in the range 1 to 200. • enable – Enables the Enhance Beacon Table feature for AP locationing. • erase-report – Erases the reports for Enhanced Beacon Table feature. • max-ap <0-512> – Sets the maximum number of APs to be recorded in the Enhanced Beacon Table. Set a value in the range 0 -512. • scan-interval <10-60> – The time duration between two enhanced beacon table for AP locationing scans in seconds. • scan-time <100-1000> – The time duration of an Enhanced Beacon Table scan in milliseconds. • enhanced-probe-table [enable|erase-report|max-mu|preferred|window-time] – Enhanced probe table for MU locationing. • enable – Enables the Enhanced Probe Table feature for MU locationing. • erase-report – Erases the reports for Enhanced Probe Table feature. • max-mu <0-512> – Sets the maximum MUs in the Enhance Probe Table report. • preferred <MAC> – Add the MAC <MAC> to the preferred MU list. • window-time <10-60> – Sets the Window Time for probe collection in seconds to a value in the range 10 to 60 seconds.

	• free-packet-watermark <0-100>– The free packets threshold in percent. If the percentage of free packets is lower than this number, then additional packets will not be queued in the datapath. • idle-radio-send-multicast enable – Enables forwarding multicast packets to radios without associated mobile units. • legacy-load-balance – Invoke legacy load balance algorithm. • map-radios <1-127> – Sets radio-to-cpu mapping constant to a value in the range of 1 and 127. • radio-misc-cfg <hex-bitmask> – Radio specific miscellaneous U16 configuration for all radios. • rate-scale – Enable wireless rate scaling (default). • request-ap-log <1-1024> – Request AP Log for the selected AP. • save-ap-log – Saves debug/error logs sent by the access-port • snmp-trap-throttle <1-20> – Limits the number of SNMP traps generated per second from the wireless module to a number in the range 1 and 20. • sync-radio-entries – sync radio configuration at cluster levels. • vlan-cache enable – Enables VLAN-cache mode.

See also, *Chapter 2, Section 2.1.5 service* on *page 2-7*.

Usage Guidelines

To stop a service, use the no command. For instance, use **`no service wireless idle-radio-send-multicast enable`** to stop sending broadcast/multicast frames to idle radios

Example

```
RFSwitch(config-wireless)#service show wireless ap-history
AP MAC             Radio  Timestamp          Event
Reason
============================================================
=======
00-A0-F8-BF-8A-4B  N/A    20070926-20:23:10  Adoption    N/A
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#service show wireless mvlan 20
Wlan 20: pool_size =1
------------------------------------------------------
[ 0]: wlan=20, vlan_id=1, limit=0, users=0, log_sent=0
[ 1]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 2]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 3]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 4]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 5]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 6]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 7]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 8]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 9]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[10]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[11]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[12]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[13]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[14]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[15]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[16]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[17]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[18]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[19]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[20]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[21]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[22]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[23]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[24]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[25]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[26]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[27]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[28]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[29]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[30]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[31]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
```

```
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#service show wireless radio
description
# access-port MAC      start BSS          radio  description
coordinates
1] 00-A0-F8-BF-8A-4B 00-A0-F8-BF-EF-B0 11bg  RADIO1
0 0 0
2] 00-A0-F8-BF-8A-4B 00-A0-F8-BF-ED-BC 11a   RADIO2
0 0 0
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#service show wireless snmp-trap-
throttle
throttle : 10 (default = 10)
traps allowed through throttle: 9
traps dropped through throttle: 0
RFSwitch(config-wireless)#
```

20.1.48 show

Wireless Configuration Commands

Displays current system information running on the switch

For other show commands, see *Chapter 2, Section 2.2 show* on *page 2-37*.

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-wireless)#show ?
  access-list                          Internet Protocol (IP)
  aclstats                             Show ACL Statistics information
  alarm-log                            Display all alarms currently in
the system
  autoinstall                          autoinstall configuration
  banner                               Display Message of the Day Login
banner
  boot                                 Display boot configuration.
  clock                                Display system clock
  commands                             Show command lists
  crypto                               encryption module
  debugging                            Debugging information outputs
  dhcp                                 DHCP Server Configuration
  environment                          show environmental information
```

```
  file                                Display filesystem information
  firewall                            Wireless firewall
  ftp                                 Display FTP Server configuration
  history                             Display the session command
history
  interfaces                          Interface status
  ip                                  Internet Protocol (IP)
  ldap                                LDAP server
  licenses                            Show any installed licenses
  logging                             Show logging configuration and
buffer
  mac                                 Internet Protocol (IP)
  mac-address-table                   Display MAC address table
  mac-name                            Displays the configured mac
names
  management                          Display L3 Managment Interface
name
  mobility                            Display Mobility parameters
  ntp                                 Network time protocol
  password-encryption                 password encryption
  port                                Physical/Aggreagte port
interface

  port-channel                        Portchannel commands

  privilege                           Show current privilege level
  radius                              RADIUS configuration commands

  redundancy-                         Display redundancy group
parameters

  role                                Configure role parameters
  rtls                                Real Time Locating System
commands
  running-config                      Current Operating configuration
  securitymgr                         Securitymgr parameters
  sessions                            Display current active open
connections
  smtp-notification                   Display SNMP engine parameters
  snmp                                Display SNMP engine parameters
  snmp-server                         Display SNMP engine parameters
  spanning-tree                       Display spanning tree information
  startup-config                      Contents of startup configuration
  static-channel-group                static channel group membership
  terminal                            Display terminal configuration
parameters
  timezone                            Display timezone
  traffic-shape                       Display traffic shaping
  upgrade-status                      Display last image upgrade status
  users                               Display information about
currently logged in users
  version                             Display software & hardware
version
```

```
  wireless                          Wireless configuration commands
  wlan-acl                          wlan based acl

RFSwitch(config-wireless)#show

RFSwitch(config-wireless)#show wireless config
country-code            : us
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : disabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix broadcast-rsp  : disabled
broadcast-tx-speed      : optimize-for-range
wlan bw allocation      : enabled
Adaptive ap parameters:
 config-apply def-delay : 30 seconds
 config-apply mesh-delay: 3 minutes
wired-to-wireless rate limit per user : unlimited
wireless-to-wired rate limit per user : unlimited
user load balance mode  : by-throughput
.............................................................
..
.............................................................
..
.............................................................
..
RFSwitch(config-wireless)

RFSwitch(config-wireless)#show wireless radio-group
 group_id   | radios
 ------------------------------------------------------------
         11 | 1,4
RFSwitch(config-wireless)#
```

20.1.49 smart-rf

Wireless Configuration Commands

Configures Smart-RF Management parameters and moves to the `(config-wireless-smart-rf)` instance

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: `smart-rf` initiates the`(config-wireless-smart-rf)` instance. For more details see *Chapter 25, Smart RF Instance*. The prompt changes from `RFSwitch (config-wireless)#` to `RFSwitch (config-wireless-smart-rf)`

Syntax

`smart-rf`

Parameters

None

Example

```
RFS7000(config-wireless)#smart-rf
RFS7000(config-wireless-smart-rf)#
```

20.1.50 smart-scan-channels

Wireless Configuration Commands

Specifies a list of channels for Motorola clients to do smart-scan

Syntax

```
smart-scan-channels [<channel-list>|add <channel-list>|
  remove <channel-list>]
```

Parameters

<channel-list>	A comma-separated list of channels
add <channel-list>	Add one or more channels to existing channel list
remove <channel-list>	Remove one or more channels from existing channel list

Example

```
RFS7000(config-wireless)#smart-scan-channels add 1,3,4
```

20.1.51 wlan

▸ *Wireless Configuration Commands*

Configures Wireless LAN related commands

Syntax

```
wlan [<1-256>|<wlan-list>] [80211-extensions|
  aap-proxy-radius|accounting|acl|add-vlan|answer-bcast-ess|
  authentication-type|client-bridge-backhaul|description|
  dot11i|enable|encryption-type|hold-time|hotspot|
  inactivity-timeout|independent|ip|kdc|mobility|
  mu-mu-disallow|nac-mode|nac-server|nas-id|nas-port-id|
  qos|radius|secure-beacon|set-vlan-user-limit|
  smart-scan-channels|ssid|storm-control|syslog|vlan|wep128|
  wep64]
wlan <1-256> [answer-bcast-ess|enable|independent|
  mu-mu-disallow

wlan <1-256> 80211-extensions move-command enable
wlan <1-256> aap-proxy-radius enable realm <realm name>
  strip
wlan <1-256> accounting [none|radius|ssyslog]
wlan <1-256> acl exceed-rate mu-denied-traffic <0-10000000>
  disassociate
wlan <1-256> add-vlan [<1-4094>|<vlan-list>]
  {limit <0-4096>}
wlan <1-256> authentication-type [eap|hotspot|kerberos|
  mac-auth|none]
wlan <1-256> client-bridge-backhaul enable
wlan <1-256> description <description>

wlan <1-256> dot11i [handshake|key|key-rotation|
  key-rotation-interval|opp-pmk-caching|phrase|pmk-caching|
  preauthentication|second-key|tkip-cntrmeas-hold-time|
  wpa2-tkip]
wlan <1-256> dot11i [opp-pmk-caching|pmk-caching|
  preauthentication
wlan <1-256> dot11i handshake timeout <100-5000>
  retransmit <1-10>
wlan <1-256> dot11i key [0 <secret-key>|2 <secret-key>|
  <secret-key>]
wlan <1-256> dot11i key-rotation enable
wlan <1-256> dot11i key-rotation-interval <30-86400>
wlan <1-256> dot11i phrase [0 <secret-key>|2 <secret-key>|
  <secret-key>]
```

```
wlan <1-256> dot11i second-key [enable|key|phrase]
wlan <1-256> dot11i second-key enable
wlan <1-256> dot11i second-key [key|phrase] [0 <secret-key>|
  2 <secret-key>|<secret-key>]
wlan <1-256> dot11i tkip-cntrmeas-hold-time <0-65535>
wlan <1-256> dot11i wap2-tkip enable

wlan <1-256> encryption-type [ccmp|keyguard|none|tkip|
  tkip-ccmp|wep128|wep128-keyguard|wep64]
wlan <1-256> hold-time <1-300>

wlan <1-256> hotspot [allow-eap|allow-list|cache-ageout|
  ntf-logout-port|query|redirect-to-hostname|
  simultaneous-users|webpage|webpage-location]
wlan <1-256> hotspot [allow-eap|redirect-to-hostname
wlan <1-256> hotspot allow-list <1-32> <IP>
wlan <1-256> hotspot cache-ageout <5-86400>
wlan <1-256> hotspot ntf-logout-port <0-65535>
wlan <1-256> hotspot simultaneous-users <0-8192>
wlan <1-256> hotspot webpage [external|internal]
  [failure|login|welcome] <URL>
wlan <1-256> hotspot webpage-location
  [advanced|external|internal {logout-on-browser-close}]

wlan <1-256> inactivity-timeout <60-86400>

wlan <1-256> ip [arp|dhcp]
wlan <1-256> ip arp [rate-limit <1-1000000>|trust]
wlan <1-256> ip dhcp trust

wlan <1-256> kdc [password|realm|server]
wlan <1-256> kdc password [0 <secret>|2 <secret>|<secret>]
wlan <1-256> kdc realm <realm>
wlan <1-256> kdc server [primary|secondary|timeout]
wlan <1-256> kdc server primary <IP> {auth-port <port>}
wlan <1-256> kdc server secondary <IP> {auth-port <port>}
wlan <1-256> kdc server timeout <1-60>

wlan <1-256> mobility enable

wlan <1-256> nac-mode [bypass-nac-except-include-list|
  do-nac-except-exclude-list|none]
wlan <1-256> nac-server [primary|secondary|timeout]
```

```
wlan <1-256> nac-server [primary|secondary]
  [<IP> {auth-port <port>}|radius-key [0 <secret>|
  2 <secret>|<secret>]]
wlan <1-256> nac-server timeout <1-300> retransmit <1-100>

wlan <1-256> nas-id <nas-id>
wlan <1-256> nas-port-id <port>

wlan <1-256> qos [classification|mcast-with-dot11i|mcast1|
  mcast2|prioritize-voice|rate-limit|svp|weight|wmm]
wlan <1-256> qos classification [low|normal|video|voice|wmm]
wlan <1-256> qos mcast-with-dot11i enable
wlan <1-256> qos [mcast1|mcast2] <MAC>
wlan <1-256> qos prioritize-voice
wlan <1-256> qos rate-limit [wired-to-wireless|
  wireless-to-wired] <100-1000000>
wlan <1-256> qos svp enable
wlan <1-256> qos weight <1-10>
wlan <1-256> qos wmm [8021p|background|best-effort|dscp|
  video|voice]
wlan <1-256> qos wmm [8021p|dscp]
wlan <1-256> qos wmm [background|best-effort|video|voice]
[aifsn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>]

wlan <1-256> radius [accounting|authentication-protocol|
  dscp|dynamic-authorization|dynamic-vlan-assignment|
  mac-auth-format|mobile-unit|reauth|server]
wlan <1-256> radius accounting [mode|server|timeout]
wlan <1-256> radius accounting mode [start-interim-stop
  interval <60-3600>|start-stop|stop-only]
wlan <1-256> radius accounting server [primary|secondary]
[<IP> {acct-port <port>}|radius-key [0 <key>|2 <key>|<key>]]
wlan <1-256> radius accounting timeout <1-60> retransmit
  <1-100>
wlan <1-256> radius authentication-protocol [chap|pap]
wlan <1-256> radius dscp <0-63>
wlan <1-256> radius [dynamic-authorization|
  dynamic-vlan-assignment] enable
wlan <1-256> radius mac-auth-format [no-delim|pair-colon|
  pair-dash|quad-dot|middle-dash]
wlan <1-256> radius mobile-unit timeout <1-10>
  retransmit <1-10>
wlan <1-256> radius reauth <30-65535>
wlan <1-256> radius server [primary|secondary|timeout]
```

```
wlan <1-256> radius server [primary|secondary] [<IP>
  {auth-port <1024-65535>}|radius-key [0 <key>|2 <key>|
  <key>]
wlan <1-256> radius server timeout <1-60> retransmit <1-10>

wlan <1-256> secure-beacon
wlan <1-256> set-vlan-user-limit [<1-4094>|<vlan-list>]
  <0-8192>
wlan <1-256> smart-scan-channels [<channel-list>|add
<channel-list>|remove <channel-list>]
wlan <1-256> ssid <ssid>
wlan <1-256> storm-control [bcast|mcast|ucast]
  rate-limit <1-1000000>
wlan <1-256> syslog accounting server <IP> {port <1-65535>}

wlan <1-256> vlan [<1-4094>|<vlan-list>] {limit <0-8192>}

wlan <1-256> [wep64|wep128] [key|phrase|wep-default-key]
wlan <1-256> [wep64|wep128] key <1-4> [ascii|hex]
  [0 <key>|1 <key>|<key>]
wlan <1-256> [wep64|wep128] phrase <pass-phrase>
wlan <1-256> [wep64|wep128] wep-default-key <1-4>
```

Parameters

<1-256>	Defines a single WLAN index
<wlan-list>	Sets a list (1,3,7) or range (3-7) of WLAN indices

For each of the options <1-256> and <wlan-list> the following commands are available.

80211-extensions move-command enable	Enables support for 802.11 extensions. • move-command – Enables support for fast roaming. • enable – Enables this extension.
aap-proxy-radius enable realm <realm-name> strip	Enables configuring of proxying AAP RADIUS requests. • realm <realm-name> – Provide proxy realm name. • strip – Strip realm name while proxying requests.

accounting [none|radius|syslog]	Defines the accounting configuration on this WLAN. • none – No accounting performed on this WLAN. • radius – Uses RADIUS accounting on this WLAN. • syslog – Uses Syslog accounting on this WLAN.
acl exceed-rate mu-denied-traffic <0-1000000> disassociate	Sets the actions taken based on the ACL configuration. • exceed-rate – Action is taken when rate exceeds a set value. • mu-denied-traffic – The action is to deny traffic to the MU. • <0-1000000> – The rate of packets / second after exceeding which the traffic from the MU is denied access. • disassociate – When enabled, the MU is disassociated.
add-vlan [<1-4094>|<vlan-list>] *{limit <1-4094>}*	Instead of starting a new VLAN assignment for given WLAN, this command adds a VLAN assignment to an existing VLAN assignment. All prior VLAN settings are retained. • [<1-4094>|<vlan-list>] – Sets the VLAN range list <vlan-list>. It can be either a single index or a list (1,3,7) or range (3-7). • limit – Sets user limits on VLANs to a value in the range <1-4094> for this WLAN. **Note:** The `[no]` form of `add-vlan` command deletes the specified VLAN mapping over the specified WLAN range list. If the specified mapping does not exist for a particular WLAN, a "specified vlan does not exists" message displays. The delete action continues on remaining VLANs. If all the VLANs are deleted a default VLAN assignment takes effect.
answer-bcast-ess	Allows this WLAN to respond to probes for broadcast ESS.

authentication-type [eap|hotspot|kerberos| mac-auth|none]	Sets the authentication type for this WLAN. • eap – EAP authentication (802.1X). • hotspot – Web based authentication. • kerberos – Kerberos authentication (encryption will change to WEP128 if its not already wep128/keyguard). • mac-auth – MAC authentication (RADIUS lookup of MAC address). • none – No authentication is used.
client-bridge-backhaul enable	Enables the client bridge backhaul capability on this wlan.
description <description>	Sets the description for this WLAN. Use to identify the selected WLAN.

dot11i [handshake | key| key-rotation | key-rotation-interval| opp-pmk-caching | phrase|pmk-caching | preauthentication | second-key| tkip-cntrmeas-hold-time| wpa2-tkip]	Modifies tkip/ccmp (802.11i) related parameters. • handshake timeout <100-5000> retransmit <1-10> – Sets a handshake for the timeout and retransmission intervals. • timeout <100-5000> – Sets the timeout (in milliseconds) between retries. • retransmit <1-10> – Sets the number of retransmission attempts. • key [0 <secret-key>|2 <secret-key>|<secret-key>] – Configure the key (PMK). • 0 <secret-key>– Password is specified unencrypted. • 2 <secret-key>– Password is encrypted with password-encryption secret. • <secret-key> – The 256bit (64 hex characters) long key. • key-rotation enable – Controls the periodic update of broadcast keys for associated mobile units. • key-rotation-interval <30-86400> – Configures the broadcast key rotation interval in seconds. • opp-pmk-caching – Enables the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X). • phrase [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the passphrase. • 0 <secret-key> – Password is specified unencrypted. • 2 <secret-key> – Password is encrypted with password-encryption secret. • <secret-key> – Set a passphrase between 8 and 63 characters. • pmk-caching – Enables the use of cached pairwise master keys (fast roaming with eap/802.1X). • preauthentication – Enables support for 802.11i pre-authentication.

	• second-key [enable|key|phrase] – Configures a secondary set of key/passphrase for this WLAN. • enable – Enables the use of a secondary key/passphrase. • key [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the key (PMK). • phrase [0 <secret-key>|2 <secret-key>|<secret-key>] – Configures the passphrase. • 0 <secret-key>– Password is specified as unencrypted. • 2 <secret-key>– Password is encrypted with password-encryption secret. • <secret-key> – Sets the 256bit (64 hex characters) key. • tkip-cntrmeas-hold-time <0-65535> – Configures the hold-time (in seconds) that clients are blocked when TKIP counter measures are invoked. Default is 60 seconds. • wpa2-tkip enable – Enables support for WPA2-TKIP (in addition to WPA-TKIP) when TKIP is enabled on this WLAN.
enable	Enables specified WLAN(s).

encryption-type [ccmp|keyguard| none|tkip|tkip-ccmp| wep128|wep64| web128-keyguard]	Sets the encryption type for this WLAN. Options include: • ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM CCMP). • keyguard – Keyguard-MCM (Mobile Computing Mode). • none – No encryption. • tkip – Enables *Temporal Key Integrity Protocol* (TKIP). • tkip-ccmp – Enables both TKIP and CCMP on this WLAN. • wep128 – Enables *Wired Equivalence Privacy* (WEP) with 128 bit keys. • wep128-keyguard – Enables WEP128 as well as Keyguard-MCM on this WLAN. • wep64 – Enables *Wired Equivalence Privacy* (WEP) with 64 bit keys. **Note:** A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption and the other uses WEP.
hold-time <1-300>	Specifies the time duration in seconds to hold user credentials when a MU leaves or roams out.

hotspot [allow-eap| allow-list|cache-ageout| ntf-logout-port| redirect-to-hostname| simultaneous-users| query|webpage| webpage-location)	Modifies hotspot related parameters • allow-eap – allow EAP authentication in addition to web based login. • allow-list <1-32> <IP> – Specifies the allowed list that user can access without prior authentication. Typically this would be the external web-page's IP address. • <1-32> – Allow-list Rule index value. • <IP> – Allow-list IP address. This parameter refers to a specific IP address to which unauthenticated mobile-units can connect to. It does not specify a network or a subnet. • cache-ageout <5-86400> – The time duration in seconds to ageout the cache after MU disassociation. • ntf-logout-port <0-65535> – Configures the port to send the NTF-Logout when the device is in external hotspot mode. • max-login-attempts <0-10> – Modifies hotspot maximum login attempts. • <0-10> – Login attempts between 0-10. • query [<1-10>|<query-list>] – Specifies queries to be appended to redirection URL. • <1-10> – A single index. • <query-list> – A list of indices. • redirect-to-hostname – Use the Hostname/System-Name in the redirection URL instead of the IP address of the switch. • simultaneous-users <0-8192> – Specifies how many simultaneous MAC address can be allowed for a given end user. • <0-8192> – The number of MAC addresses that are allowed to use that username at the same time. 0 implies disabling of the checks.

	• webpage external [failure|login|welcome] <URL> – Modifies hotspot page parameters.
	• external – Modifies a hotspot's External Web page.
	• failure – When login fails.
	• login – When login succeeds.
	• welcome – The page to display to welcome user.
	• <URL> – Sets the path to the file to be displayed.
	Note: When using authentication server, the URL parameters ip_address and port are required when the external entity that serves the pages and authentication server are not the same.
	`http://<external_url> <login|welcome|fail>.html?ip_address=<a.b.c .d>&port=<x>`
	`where:`
	• <url> is the url of the server serving the web pages
	• <login|welcome|fail>.html is the name of the file to be served
	• ip_address=<a.b.c.d> is the IP address of the authentication server. The default ip_address is the same as the IP of the server that is serving the pages
	• port=<x> is the port on the authentication server. The default port is 444.
	• internal – Modifies hotspot's Internal Web pages. The following page parts can be defined and modified. You can enter upto 1024 characters for each parameter.
	• description – The description of the page.
	• footer – The footer for the page.
	• header - The page header.
	• main-logo – The main logo for the page.
	• small-logo – A small logo for the page.
	• title – The page title.

	Note: The full syntax for the internal page definition is as follows: • `wlan 1 hotspot webpage internal welcome title Welcome to hotspot page. You have logged on successfully`failure – Users are redirected to this Web page if they fail authentication. File must be named *fail.html*. • login – Users are prompted for their username and password within this Web page. File must be named *login.html.* • welcome – Users are redirected to this Web page after they authenticate successfully. File must be named *welcome.html.* • webpage-location [advanced|external|internal] – The location of the Web pages used for authentication. These pages can either be hosted on the switch or an external Web Server. • advanced – Invokes login/welcome/failure Web pages created by the user on the switch. • external – Invokes login/welcome/failure Web pages on an external server. • internal (logout-on-browser-close)– Invokes login/ welcome/failure Web pages created automatically on the switch. • logout-on-browser-close – Enables/disables user logout on browser close. Default value `disable.`

ip [arp|dhcp]	Sets Internet Protocol settings for ARP and DHCP packets. • arp [rate-limit <1-1000000>|trust] – Address Resolution Protocol configuration. • dhcp trust – Dynamic Host Resolution Protocol configuration. • trust – Sets the arp/dhcp responses as trusted for this wlan/range. • rate-limit <1-1000000> – Does packet rate limiting on ARP packets to a value in the range 1 and 1000000.
inactivity-timeout <60-86400>	Sets an inactivity timeout in seconds. If a frame is not received from a mobile unit for this amount of time, the mobile unit is disassociated.
independent	Sets this WLAN to be an independent WLAN.

kdc [password|realm|server]	Modifies KDC related parameters. • password [0 <secret>|2 <secret>|<secret>] – Create a KDC server password (up to 127 characters) • 0 <secret>– Password is specified unencrypted. • 2 <secret>– Password is encrypted with a password-encryption secret. • <secret> – Defines a KDC server password (up to 127 characters). • realm <realm> – Defines a KDC realm (up to 127 characters). • <realm> – Defines KDC realm (up to 127 characters) • server [primary|secondary|timeout] – Modifies KDC server parameters. • primary <IP> {auth-port <port>} – Defines the primary KDC server. • secondary <IP> {auth-port <port>}– Defines the secondary KDC server. • <IP> – Sets the KDC server IP address • auth-port <port> – Optional. Sets the KDC server authentication port to a value in the range 1 to 65535. Default is 88. • timeout <1-60> – Modifies KDC server parameters. • <1-60> – Defines the time the switch waits for a response from the KDC Server before retrying.
mobility enable	Enables L3 Mobility on WLAN(s).
mu-mu-disallow	Disallows frames from one mobile unit to another mobile unit on this WLAN.

nac-mode [bypass-nac-except-include-list| do-nac-except-exclude-list|none]	Sets the *Network Access Control (*NAC) mode configuration • bypass-nac-except-include-list – No MU NAC check is done except for those in include list. Devices in the include list have NAC checks. • do-nac-except-exclude-list – A MU NAC check is done except for those in the exclude list. Devices in the exclude list will not have any NAC checks. • none – NAC disabled, no NAC is done. An MU can only get authenticated by a Radius server.

nac-server [primary|secondary| timeout]	Configure a NAC server IP address and an optional authentication port number. • [primary|secondary] [<IP> {auth-port <port>}|radius-key [0 <secret>|2 <secret>|<secret>]] – Primary server or secondary server's IP address • <IP> {auth-port <port>} – Set an EAP server IP address and optional EAP server authentication port (default: is 1812) • radius-key [0 <secret>|2 <secret>|<secret>] – Create a Radius server shared secret, up to 127 characters • 0 <secret> – Password is specified as unencrypted • 2 <secret> – Password is encrypted with password-encryption secret • <secret> – Configures a NAC server shared secret • timeout <1-300> retransmit <1-100> – Sets the time the switch waits for a response from the RADIUS server before retrying. This is a global setting for both the primary and secondary servers. • retransmit <1-100> – Number of retries before the wireless switch will give up and disassociate mobile unit • <1-100> – Retry count **Note:** The `RFSwitch(config-wireless)# nac-server timeout<*> retransmit<*>` should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fallback to the secondary server will not work.
nas-id <nas-id>	The nas-id of this wlan to be sent to the RADIUS server. Maximum length of 256 characters.
nas-port-id <port>	The nas-port-od of this wlan to be sent to the RADIUS server. Maximum length of 256 characters.

qos [classification | mcast-with-dot11i| mcast1|mcast2| prioritize-voice| rate-limit|svp|weight| wmm]	Quality of Service commands. • classification [background|best-effort|video|voice|wmm] – Select how traffic on this WLAN is classified (relative prioritization on the access port). • low – All traffic on this wlan is treated as low priority traffic (Background). • normal – All traffic on this wlan is treated with normal priority (Best Effort). • video – All traffic on this wlan is treated as Video. • voice – All traffic on this wlan is treated as Voice. • wmm – Use WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues. • mcast-with-dot11i enable – Enables multicast mask with dot11i. • [mcast1|mcast2] <MAC> – Sets multicast masks. • mcast1 <MAC> – Sets multicast mask for egress prioritization. • mcast2 <MAC> – Sets multicast mask for egress prioritization. • <MAC> – MAC address. • prioritize-voice – Prioritize voice frames over general data frames (applies to non-WMM mobile-unit).

	• rate-limit [wired-to-wireless|wireless-to-wired] <100-1000000> – Sets traffic rate limit for users on the selected WLAN. • wired-to-wireless – Down link direction - from network to wireless client. • wireless-to-wired – Up link direction - from wireless client to network. • <100-1000000> – The rate to limit to in kbps. • svp enable – Enables support for Spectralink Voice Prioritization. • weight <1-10> – The egress weight (relative priority to other WLANs) of this WLAN. The weight sets the priority for the packets to be sent. • wmm [8021p|background|best-effort|dscp|video|voice] – Sets the 802.11e / Wireless Multi Media (WMM) parameters (supported on AP300 & AAP5131). • 8021p – Use 802.1p frame priority (field in the VLAN tag) to determine packet priority. • dscp –Use *Differentiated Services Code Point* (DSCP) bits in the IP header to determine packet priority • background [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for background traffic. • best-effort [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for normal traffic. • video [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for video traffic. • voice [aisfn <2-15>|cw <0-15> <0-15>|txop-limit <0-65535>] – Sets the parameters for voice traffic.

	• aisfn <2-15> – *Arbitration Inter Frame Spacing Number* (AIFSN) is the wait time in milliSeconds between data frames. This value is derived using AIFSN and the slot-time. • <2-15> – The AIFSN spacing number. • cw <0-15> <0-15> – *Contention Window* (CW) parameters. Wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window value. • <0-15> – CW minimum value. The actual value used is (2^ECWmin - 1) • <0-15> – CW maximum value. (2^ECWmax - 1). • txop-limit <0-65535> – The transmit-opportunity is an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium. • <0-65535> – The transmit-opportunity in 32 microSecond units.

radius [accounting| authentication-protocol| dscp| dynamic-authorization| dynamic-vlan-assignment| mac-auth-format| mobile-unit| reauth|server]	Configures RADIUS parameters for the select WLAN. • accounting [mode|server|timeout] – Sets RADIUS accounting parameters. • mode [start-stop|stop-only|start-interim-stop] – Sets the Accounting Mode. • start-stop – Sends accounting start-stop. • stop-only – Sends accounting stop-only. • start-interim-stop interval <60-3600> – Sets the time interval between successive accounting updates to a value in the range 60 to 3600 secs. • server [primary|secondary] [<IP> *{acct-port <port>}*| radius-key [0 <key>|2 <key>|<key>]] – Sets the primary or secondary RADIUS server for the selected WLAN. • primary – Sets primary RADIUS server information. • secondary – Sets secondary RADIUS server information. • <IP> – Sets the IP address of the RADIUS server. • acct-port <port> – Sets the optional radius server accounting port. Default is 1813. • radius-key [0 <key>|2 <key>|<key>] – Sets the radius-key for the RADIUS server. • 0 <key> – The key is sent unencrypted. • 2 <key> – The key is sent encrypted with the password-encryption secret. • <key> – The shared key. • timeout <1-300> – Sets the time the wireless switch waits for a response from the RADIUS server before retrying accounting. • <1-300> – The time duration in seconds.

	• authentication-protocol [chap|pap] – Sets the RADIUS Authentication Protocol for RADIUS request. Select from CHAP or PAP. • dscp <0-63> – Specify a *Differentiated Services Code Point* (DSCP) value to provide QoS to RADIUS packets. Set a value in the range 0 to 63. • dynamic-authorization enable – Configures support for RADIUS dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576. • enable – Enables this feature. • dynamic-vlan-assignment enable – Allow users to be assigned to RADIUS server specified VLANs, instead of only the vlan that is mapped to this wlan. • enable – Enables this feature. • mac-auth-format [no-delim|pair-colon|pair-dash|quad-dot|middle-dash] – Set the MAC address format to use. • middle-dash – Dash Delimiter in the middle - AABBCC-DDEEFF • no-delim – No Delimiter - AABBCCDDEEFF • pair-colon – Colon Delimiter per Pair - AA:BB:CC:DD:EE:FF • pair-dash – Dash Delimiter per Pair - AA-BB-CC-DD-EE-FF • quad-dot – Dot Delimiter per Four Hex - AABB.CCDD.EEFF • mobile-unit timeout <1-300> retransmit <1-100> – Modifies RADIUS/802.1X supplicant related parameters. • timeout <1-300> – Sets the Time the wireless switch waits for a response from the mobile-unit before retrying. Set a value in the range 1 to 300. • retransmit <1-100> – Sets the number of retries before the wireless switch will give up and disassociate the mobile-unit. Set a value in the range 1 to 100.

	• server [primary|secondary] [<IP> *{acct-port <port>}*| radius-key [0 <key>|2 <key>|<key>]] – Sets the primary or secondary RADIUS server for the selected WLAN. • primary – Sets primary RADIUS server information • secondary – Sets secondary RADIUS server information. • <IP> – Sets the IP address of the RADIUS server. • acct-port <port> – Sets the optional radius server accounting port. Default is 1813. • radius-key [0 <key>|2 <key>|<key>] – Sets the radius-key for the RADIUS server. • 0 <key> – The key is sent unencrypted. • 2 <key> – The key is sent encrypted with the password-encryption secret. • <key> – The shared key. • timeout <1-300> retransmit <1-100> – Sets the time the switch waits for a response from the RADIUS server before retrying. This is a global setting for both the primary and secondary servers. • retransmit <1-100> – Number of retries before the wireless switch will give up and disassociate mobile unit • <1-100> – Retry count • reauth <30-65535> – Enable periodic reauthentication of all associated mobile-units. • <30-65535> – The reauthentication interval in seconds.
secure-beacon	Does not include the SSID of this WLAN in beacon frames
set-vlan-user-limit [<1-4094>|<vlan-list>] <0-8192>	Sets user limits on VLANs for this WLAN • [<1-4094>|VLAN] – VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7) of indices • [<0-8192>] – Sets the VLAN index. The limit is <0-8192>

smart-scan-channels [<channel-list>| add <channel-list>| remove <channel-list>]	Specifies a list of channels to motorola clients to perform a smart-scan. The following are the options set: • <channel-list> – A comma separated list of channels to scan. Can also contain a single channel number. • add <channel-list> – Adds the specified channel(s) to the smart-scan list. • remove <channel-list> – Removes the specified channel(s) from the smart-scan list.
ssid <ssid>	Enter the SSID of this WLAN. <ssid> can be up to 32 characters.
storm-control [bcast|mcast|ucast] rate-limit <rate>	Enables packet dropping in case of flooding attack. • bcast – broadcast packets • mcast – multicast packets • ucast – unicast packets • rate-limit <rate>– Enables rate limiting if the rate exceeds the value set by <rate> (1-1000000 packets/ second).
syslog accounting server <IP> *{port <1-65535>}*	Syslog Accounting • accounting – Modifies accounting parameters • server <IP> – Modifies the Syslog accounting server IP Address. • port <1-65535> – Optional. Defines the Syslog server port. The default port number is 514 .
vlan [<1-4094>| <vlan-list>] *{limit <0-8192>}*	Sets the VLAN assignment of this WLAN. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased. • [<1-4094>|<vlan-list>] –Establishes the VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7). • limit <0 -8192> – Sets user limits on VLANs for this WLAN.

wep128 [key|phrase| wep-default-key]	Configures WEP128 parameters. • key *<1-4>* [ascii|hex] – Configures pre-shared hex keys. • ascii [0 <key>|1 <key>|<key>] – Sets keys as ascii characters (5 characters for wep64, 13 for wep128). • hex [0 <key>|1 <key>|<key>] – Sets keys as hexadecimal characters (10 characters for wep64, 26 for wep128). • 0 <key> – Password is specified unencrypted. • 2 <key> – Password is encrypted with password-encryption secret. • <key> – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128). • phrase <phrase> – Specifies a passphrase from which keys are to be derived. • <phrase> – Sets the passphrase (between 4 and 32 characters). • wep-default-key <1-4> – Defines the key index used for transmission from AP to MU.

wep64 [key|phrase| wep-default-key]	Configures WEP64 parameters. • key *<1-4>* [ascii|hex] – Configures pre-shared hex keys. • ascii [0 <key>|1 <key>|<key>] – Sets keys as ascii characters (5 characters for wep64, 13 for wep128). • hex [0 <key>|1 <key>|<key>] – Sets keys as hexadecimal characters (10 characters for wep64, 26 for wep128). • 0 <key> – Password is specified unencrypted. • 2 <key> – Password is encrypted with password-encryption secret. • <key> – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128). • phrase <phrase> – Specifies a passphrase from which keys are to be derived. • <phrase> – Sets the passphrase (between 4 and 32 characters). • wep-default-key <1-4> – Defines the key index used for transmission from AP to MU.

Example

```
RFSwitch(config-wireless)#wlan 25 accounting syslog
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 answer-bcast-ess
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 authentication-type
kerberos
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 description "TestWLAN"
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 dot11i handshake timeout
2500 retransmit 5
RFSwitch(config-wireless)#
```

```
RFSwitch(config-wireless)#wlan 25 dot11i key-rotation enable
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 dot11i key-rotation-
interval 2000
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 enable
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 hotspot webpage external
failure "This feature is under development"
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 kdc server primary 1.2.3.4
auth-port 50000
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 mobility enable

RFSwitch(config-wireless)#wlan 1 nac-mode bypass-nac-except-
include-list
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 1 nac-server primary
11.22.33.22 auth-port 1221
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 radius accounting timeout
30 retransmit 50
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 radius mobile-unit timeout
30 retransmit 5
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 ssid TestString
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 25 symbol-extensions fast-
roaming enable
RFSwitch(config-wireless)#
```

```
RFSwitch(config-wireless)#wlan 25 syslog accounting server
12.13.14.125 port 5005
RFSwitch(config-wireless)#

RFSwitch(config-wireless)#wlan 24 qos mcast-with-dot11i
enable
RFSwitch(config-wireless)#wlan 24 storm-control bcast rate-
limit 20000
```

20.1.52 wlan-bw-allocation

Wireless Configuration Commands

Enables WLAN bandwidth allocation on all radios

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
wlan-bw-allocation enable
```

Parameters

enable	Enables WLAN bandwidth allocation on all radios.

Example

```
RFSwitch(config-wireless)#wlan-bw-allocation enable
RFSwitch(config-wireless)#
```

21

RTLS Instance

Use the `(config-rtls)` instance to configure *Real Time Location System* (RTLS) parameters.

To navigate to this instance, use the command

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#
```

21.1 RTLS Config Commands

This summarizes **`config-rtls`** commands:

Command	*Description*	*Ref.*
aeroscout	Configures aeroscout parameters	*page 21-3*
clear	Clears locationing information	*page 21-4*
clrscr	Clears display window	*page 21-5*
end	Ends the current mode and moves to EXEC mode	*page 21-6*
espi	Configures ESPI parameters	*page 21-7*
exit	Ends current mode and moves to the previous mode	*page 21-8*
help	Description of the interactive help system	*page 21-9*
ekahau	Configures ekahau parameters	*page 21-10*

Command	***Description***	***Ref.***
no	Negates a command or sets its defaults	*page 21-11*
reference-tag	Configures reference tags	*page 21-14*
rfid	Configures RFID readers	*page 21-16*
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 21-17*
show	Displays the running system information	*page 21-20*
site	Configures site parameters	*page 21-23*
sole	Configures *Smart Opportunistic Location Engine* (SOLE) parameters	*page 21-25*
switch	Configures switch parameters	*page 21-26*
zone	Configures zone	*page 21-27*
ap	Configures AP specific RTLS parameters	*page 21-28*

21.1.1 aeroscout

RTLS Config Commands

Configure support for Aeroscout RTLS engine.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
aeroscout [enable|multicast-listen-addr<MAC-Address>]
```

Parameters

enable	Enables and configures external Aeroscout RTLS engine
multicast-listen-addr <MAC-Address>	Configures multicast MAC address to which Aeroscout tags packets are destined • <MAC-Address> – Multicast MAC address. AeroScout's default multicast MAC address is '01:0C:CC:00:00:00'.

Usage Guidelines

Use `[no] aeroscout (enable)` to disable support for Aeroscout RTLS engine. This does not affect on-board locationing.

Example

```
RFSwitch(config-rtls)#aeroscout enable
RFSwitch(config-rtls)#
```

21.1.2 clear

RTLS Config Commands

Clears tags/assets information associated with aeroscout, mu, rfid and/or zone.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clear rtls tags[aeroscout|mobile-unit|ekahau|rfid|zone
<1-48>]
```

Parameters

rtls tags [aeroscout |mobile-unit|ekahau |rfid|zone <1-48>]	Real time locationing configuration • tags – Clears tag/asset information for: • aeroscout – Clears Aeroscout tags • g2 – Clear g2 tags • mobile-unit – Clears mobile-unit(wi-fi clients) • ekahau – Clears ekahau tags • rfid – Clears passive RFID tags • zone <1-48> – Clears tags in specified zone

Example

```
RFSwitch(config-rtls)#clear rtls tags aeroscout
RFSwitch(config-rtls)#
```

21.1.3 clrscr

RTLS Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-rtls)#clrscr
RFSwitch(config-rtls)#
```

21.1.4 end

RTLS Config Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-rtls)#end
RFSwitch#
```

21.1.5 espi

RTLS Config Commands

Configures *Enterprise Services Programming Interface* (ESPI) related parameters



NOTE: `espi` command instantiates `(config-rtls-espi)` sub-instance. For more details see *ESPI Instance on page 22-1*. The prompt changes from `RFSwitch(config-rtls)#` to `RFSwitch(config-rtls-espi)`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`espi`

Parameters

None

Example

```
RFSwitch(config-rtls)espi
RFSwitch(config-rtls-espi)
```

21.1.6 exit

RTLS Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-rtls)#exit
RFSwitch(config)#
```

21.1.7 help

RTLS Config Commands

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-rtls)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-rtls)#
```

21.1.8 ekahau

RTLS Config Commands

Enables and configures the external ekahau location engine

- RFS7000
- RFS600

Syntax

```
ekahau [enable|engine ip<IP> port<Port>|multicast-listen-
addr<MAC>]
```

Parameters

enable	Enables and configures external ekahau RTLS engine
`engine ip<IP> port <Port>`	Configures the IP address and port number of the external ekahau RTLS engine • ip – Configures external location engine IP address • port <1000-9000> – Configure external location engine port
multicast-listen-addr <MAC>	Configures multicast MAC address to which ekahau tags packets are destined • <MAC> – Multicast MAC address

Use `[no] enable` and `[no] engine <ip><port>` to undo the ekahau RTLS engine configuration and disable it.

Example

```
RFS7000(config-rtls)#ekahau enable
RFS7000(config-rtls)#


RFS7000(config-rtls)#ekahau engine ip 10.1.1.1 port 1001
RFS7000(config-rtls)#

RFS7000(config-rtls)#ekahau multicast-listen-addr 01-18-8E-
00-00-00
RFS7000(config-rtls)#
```

21.1.9 no

RTLS Config Commands

Negates a RTLS command or set its defaults

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [aeroscout|ekahau|reference-tag|service|site|
switch|ap|zone]
```

Parameters

aeroscout [enable| multi-cast-listen|addr]	Negates aeroscout configuration • enable – Disable SOLE adapter • multicast-listen-addr– Configure multicast listening address
ekahau [enable|engine|multicast]	Negates ekahau configuration • enable – Disable aeroscout external engine • engine –reset external location engine parameters • multicast-listen-addr– Configure multicast listening address
reference-tag [rfid]	Negates reference-tag configuration • rfid– Negates configuring rfid tag

service [filter <1-100> {length| memory-bank|offset }|inventory {<1-100>|default]	Negates service configuration for: • filter <1-100> {length|memory-bank|offset} – Negates RFID tag filter configuration for the selected index • length – Length of tag filter • memory-bank – Tag memory bank • offset – Offset into the tag memory bank • inventory [<1-100>|default] – Negates tag inventory for the selected index or the default index • filter – Configures tag filter for inventory • start – Starts tag inventory • start-trigger – Removes start trigger for tag inventory • stop-trigger – Removes stop trigger for tag inventory • zone – Configures logical reader
site	Negates site configuration
zone<1-48>	Negates zone configuration
ap [MAC Address <coordinates>]	• AA-BB-CC-DD-EE-FF – Disables access port MAC IP address • coordinates – Negates AP location configuration
switch [coordinates |geo-coordinates]	• Negates switch configuration parameters • coordinates – Negates switch coordinates configuration within the site • geo-coordinates – Negates switch geo coordinates configuration

Usage Guidelines

Use no command to undo the configurations on the parameters mentioned in the table. Refer to the parameters, within this chapter, for complete syntax.

Example

```
RFSwitch(config-rtls)#no aeroscout enable
RFSwitch
```

```
RFSwitch(config-rtls)#no ekahau enable
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#no  ekahau engine
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#no service inventory 1 zone 1
RFSwitch(config-rtls)#
```

21.1.10 reference-tag

RTLS Config Commands

Configures fixed RFID tag as reference tag and sets its coordinates within a specified location

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
reference-tag rfid <tag-id> coordinates x <0-65535> y
<0-65535> {[z<0-65535>]}{orientation [0|90|180|270]}
{range <1-50>}
```

Parameters

rfid <tag-id> coordinates x <0-65535> y <0-65535> {[z <0-65535>]} {orientation [0|90|180|270]} {range <1-50>}	Configures rfid tag as a reference tag • coordinates – Configures tag location • x <0-65535> – Configure X coordinate • y <0-65535> – Configure Y coordinate • z<0-65535> – Configure Y coordinate • orientation – Configures reference tag orientation (angles in degrees) • 0 – Increments only X • 90 – Decrements only X • 180 – Decrements only Y • 270 – Increments only Y • range <1-50> – Configures tag read range in feet.

Usage Guidelines

Use `[no] reference-tag rfid <tag-id> (coordinates x <0-65535> y <0-65535>) (orientation (0|90|180|270)) range <1-150>]` to rollback the reference-tag configuration.

Example

```
RFSwitch(config-rtls)#reference-tag rfid Symbol-Moto
coordinates x
600 y 600 orientation 180 range 40
RFSwitch(config-rtls)#
```

21.1.11 rfid

RTLS Config Commands

Configures RFID reader parameters

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: `rfid` command instantiates `(config-rtls-rfid)` sub-instance. For more details see *RFID Instance on page 23-1*. The prompt changes from `RFSwitch(config-rtls)#` to `RFSwitch(config-rtls-rfid)`

Syntax

`rfid`

Parameters

None

Example

```
RFSwitch(config-rtls)#rfid
RFSwitch(config-rtls-rfid)#
```

21.1.12 service

RTLS Config Commands

Invokes service commands to troubleshoot or debug (config-rtls) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service [filter|inventory|show]

service filter <1-100> [action|length|mask|
  memory-bank|name|offset]
service filter <1-100> action [allow|deny]
service filter <1-100> length <1-128>
service filter <1-100> mask <mask-name>
service filter <1-100> memory bank [epc|tid|uid]
service filter <1-100> name <name>
service filter <1-100> offset <0-32>

service inventory [<1-100>|default]
service inventory <1-100> [duration <0-100000>|
  filter{<1-100>|<name>}|report {current|differential}|
  round <0-10>|start|start-trigger|stop-trigger|zone]
service inventory <1-100> start-trigger [gpi port <1-65535>
  event <0-1> timeout <0-65535> |immediate|periodic
  offset <0-65535> period <0-65535> ]

service inventory <1-100> stop-trigger [duration
  <0-65535>|gpi port <1-65535> event <0-1> timeout <0-65535>
  |immediate]
service inventory <1-100> zone <1-48>

service show cli
```

Parameters

service filter <1-100> [action|length <1-128>|mask| memory-bank|name|offset<0-32>]	Configures RFID tag filter • action [allow|deny] – Configures action for tag filter. By default its configured to *allow* • length <1-128> – Configures number of bits to compare against tag mask • mask <name> – Configures tag mask for filter • memory-bank [epc|tid|uid] – Configures tag memory bank for the filter • epc – EPC memory bank • tid – TID memory bank • uid – UID memory bank • name <name> – Configures tag filter name • offset <0-32> – Configures first location of memory bank against which the tag mask is compared
service inventory <1-100> [duration <0-100000>| filter{<1-100>|<name>}|report {current|differential}| round <0-10>|start| start-trigger|stop-trigger|zone]	A single tag inventory index • duration <0-100000> – Inventory period in msecs • filter [<1-100>|<name>] – Configures the selected tags filter for inventory. • report – Set tag inventory report type • current – Reports current tag view • differential – Reports only the tags changed since previous report • round <0-10> – Sets tag inventory round size • start – Starts tag inventory

	• start-trigger – Configures start trigger for tag inventory • gpi – Configures GPI event based start trigger • port <1-65535> – Configures GPI port number • event <0-1> – Configures a boolean GPI event value that causes GPI event to trigger • timeout <0-65535> – Configures trigger1 timeout in miliiseconds • immediate – Starts tag inventory immediately • periodic – Configures periodic tag inventory • offset <0-65535> – Configures time offset in milliseconds • period <0-65535> – Configures time period in milliseconds • stop-trigger – Configures stop trigger for tag inventory • duration <0-65535> – Configures duration in milliseconds • gpi – Configures GPI event based start trigger • port <1-65535> – Configures GPI port number • event <0-1> – Configures a boolean GPI event value that causes GPI event to trigger • timeout <0-65535> – Configures trigger timeout in miliiseconds • immediate – Stops tag inventory immediately • zone <1-48> – Configures the selected logical reader
show cli	Show running system information • cli – Show CLI tree of current mode

Usage Guidelines

Use `[no] service [options]` to rollback any service related configurations.

Example

```
RFSwitch(config-rtls)#service filter 1 length 1
RFSwitch(config-rtls)#
```

21.1.13 show

RTLS Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <parameters>
show rtls [aeroscout|espi|filter|ekahau|reference-tags|
           rfid|site|sole|tags|zone]
```

Parameters

?	Suffix ? to the parameter to view its options and their related configuration details.

Usage Guidelines

Use ? at the end of each option until the final configuration is displayed.

Example

```
RFSwitch(config-rtls)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
      environment show environmental information
  file                  Display filesystem information
 firewall               Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name              Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  role                  Configure role parameters
  redundancy             Display redundancy group parameters
   t
  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
```

```
  smtp-notifications    Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration
parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently
logged                          in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFSwitch(config-rtls)#show

RFSwitch(config-rtls)#show rtls ?
  aeroscout       Aeroscout configurations
  espi            ESPI Configuration
  filter          RFID Tag Filters
  ekahau Ekahau configurations
  reference-tags  Reference tag Configurations
  rfid            RFID Configuration
  site            Site configurations
  sole            SOLE configurations
  tags            Tags/Assets (passive, active, wi-fi)
Information
  zone            Show zone statistics

RFSwitch(config-rtls)#show rtls

RFSwitch(config-rtls)#show rtls site
Site Name              : Not configured
Site Description       : Not configured
Site Unit              : feet
Site Dimension         : 0L X 0W X 0H
Site Scale Factor      : 1.000000
Switch Coordinates     : 0:0:0
Swith Geo Coordinates  : Not configured
Number of APs          : 0
RFSwitch(config-rtls)#
```

21.1.14 site

RTLS Config Commands

Configures RTLS site dimensions

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
site [description|dimension|name]
site description <description>
site dimension [unit [feet|meters]|x <1-9000> y <1-9000>
  z <0-180>]
site name <site-name>
```

Parameters

description <description>	Configures site description • <description> – Enter a description for the site
dimension [unit {feet|meters}|x <1-9000> y <1-9000> z <0-180>]	Configures site dimensions • length <value> – Configures site length. Select a value between <1-9000> if the unit is in feet, and if the unit is in meters the value will be between <1-3000> • width <value> – Configures width of the site. Select a value between <1-9000> if the unit is in feet, and if the unit is in meters the value will be between <1-3000>. • height <value> – Configures height of the site. Select a value between <0-180>, if the unit is in feet and if the unit is in meters the value will be between <0-60>unit – Configures the distance measurement unit to be used for the site • feet – Site distances measured in feet • meters – Site distances measured in meters
name <site-name>	Configures name for the site

Usage Guidelines

Use `[no] site [description |dimension|name]` to rollback the configurations made using the `site` command

Example

```
RFSwitch(config-rtls)#site description "Motorola RMZ
Ecospace,
India, 5th Floor"
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#site name "BLR-RMZ Ecospace"
RFSwitch(config-rtls)#
```

21.1.15 sole

RTLS Config Commands

Sets *Smart Opportunistic Location Engine* (SOLE) related configuration commands

This command leads you to the `(config-rtls-sole)#` sub-instance.

Supported in the following platforms:

- RFS7000
- RFS6000



NOTE: `sole` command instantiates `(config-rtls-sole)` sub-instance.
For more details see *SOLE Instance on page 24-1*.
The prompt changes from `RFSwitch(config-rtls)#` to `RFSwitch(config-rtls-sole)`

Syntax

`sole`

Parameters

None

Example

```
RFSwitch(config-rtls)#sole
RFSwitch(config-rtls-sole)#
```

21.1.16 switch

RTLS Config Commands

Configures the switch's geographical location parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
switch [coordinates|geo-coordinates]
switch coordinates x <0-65535> y <0-65535> z <0-65535>
switch geo-coordinates longitude <-180.00-80.00>
  latitude <-90.00 - 90.00>
```

Parameters

coordinates x <0-65535> y <0-65535> z <0-65535>	Configures switch coordinates within the site • x <0-65535> – Configures X coordinate • y <0-65535> – Configures Y coordinate • z <0-65535> – Configures Z coordinate
longitude <-180.00-80.00> latitude <-90.00 - 90.00>	Configures switch geographic coordinates • longitude <-180.00-180.00> – Configures longitude in degrees • latitude <-90.00-90.00> – Configures latitude in degrees

Example

```
RFSwitch(config-rtls)#switch coordinates x 121 y 121 z 135
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#switch geo-coordinates longitude 120
latitude 70
RFSwitch(config-rtls)#
```

21.1.17 zone

RTLS Config Commands

Configures the zone. Maximum of 16 zones can be configured for a site.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
zone <1-48> [name <name>|perimeter x <0-65535> y <<0-65535>]
```

Parameters

<1-48>name <name>|perimeter x <0-65535> y <<0-65535>]	Select a single zone index for configuration • name <name> – Configures name of new zone • perimeter [x y]– Configures zone perimeter coordinates • x <0-65535> – Defines X coordinate • y <0-65535> – Defines Y coordinate

Usage Guidelines

Use **{no} zone <index> [options]** to negate a zones configurations

Example

```
RFSwitch(config-rtls)#zone 1 name yard
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#zone 1 perimeter x 0 y 0
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#zone 1 perimeter x 40 y 0
RFSwitch(config-rtls)#

RFSwitch(config-rtls)#zone 1 perimeter x 40 y 100
```

21.1.18 ap

RTLS Config Commands

Configures ap coordinates

- RFS7000
- RFS6000

Syntax

```
ap <MAC> coordinates x <0-9000> y <0-9000>
  z <0-180>
```

Parameters

<MAC> coordinates x <0-9000> y <0-9000> z <0-180>	Select a single zone index for configuration • <MAC> – Configures access port MAC Address • x <0-9000> – Defines X coordinate • y <0-9000> – Defines Y coordinate • z <0-180> – Defines Z coordinate

Example

```
RFSwitch(config-rtls)#ap AA-BB-CC-DD-EE-FF x 10 y 10 z 0
RFSwitch(config-rtls)#
```

22

ESPI Instance

Use the `(config-rtls-espi)` instance to configure *Enterprise Services Programming Interface* (ESPI) related configuration commands.

To navigate to this instance, use the commands

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#espi
RFSwitch(config-rtls-espi)#
```

22.1 ESPI Config Commands

Table 22.1 summarizes **`config-rtls-espi`** commands:

Table 22.1 ESPI Config Command Summary

Command	Description	Ref.
adapter	Adapters configurations	*page 22-3*
clrscr	Clears the display screen	*page 22-4*
end	Ends the current mode and changes to the EXEC mode	*page 22-5*
exit	End the current mode and moves to the previous mode	*page 22-6*
help	Describes the interactive help system	*page 22-7*
no	Negates a command or set its defaults	*page 22-8*
service	Service Commands	*page 22-9*

Table 22.1 ESPI Config Command Summary (Continued)

Command	Description	Ref.
show	Shows running system information	page 22-10

22.1.1 adapter

ESPI Config Commands

Enables/disables a specified adapter or all adapters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
adapter ale-tcp [enable|port <3000-3100>]
```

Parameters

adapter ale-tcp [enable|port <3000-3100>]	Application side protocol implemented by adapter. • ale-tcp – ALE over TCP Adapter • enable – Activates/enables ESPI adapter • port <3000-3100> – Configures ESPI adapter listening port

Usage Guidelines

Use **`{no} adapter <adapter> enable`** to disable the specified adapter



NOTE: ALE-TCP is the only adapter shipped along with the switch.

Example

```
RFSwitch(config-rtls-espi)#adapter ale-tcp port 3040
RFSwitch(config-rtls-espi)#
```

22.1.2 clrscr

ESPI Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-rtls-espi)#clrscr
RFSwitch(config-rtls-espi)#
```

22.1.3 end

ESPI Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-rtls-espi)#end
RFSwitch#
```

22.1.4 exit

ESPI Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
exit
```

Parameters

None

Example

```
RFSwitch(config-rtls-espi)#exit
RFSwitch(config)#
```

22.1.5 help

ESPI Config Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-rtls-espi)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-rtls-espi)#
```

22.1.6 no

ESPI Config Commands

Defines the name of the adapter or disables the adapter(s)

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no adapter ale-tcp [enable|port <3000-3100>]
```

Parameters

adapter ale-tcp [enable|port <3000-3100>]	Negates ESPI adapter configurations. • adapter – Application side Protocol implemented by adapter. • ale-tcp – ALE over TCP Adapter • enable – Deactivates/disables ESPI adapter • port <3000-3100>– Configure ESPI adapter listening port

Example

```
RFSwitch(config-rtls-espi)#no adapter ale-tcp enable
RFSwitch(config-rtls-espi)#
```

22.1.7 service

ESPI Config Commands

Invokes service commands to troubleshoot or debug (`config-if`) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-rtls-espi)#service show cli
ESPI Config mode:
+-adapter
  +-ADAPTER
    +-activate [adapter ADAPTER activate]
    +-port
      +-<3000-3100> [adapter ADAPTER port <3000-3100>]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-adapter
    +-ADAPTER
      +-activate [no adapter ADAPTER activate]
+-quit [quit]
.....................................................
.....................................................
.....................................................
.....................................................
.....................................................
.....................................................
.....................................
RFSwitch(config-rtls-espi)#
```

22.1.8 show

ESPI Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-rtls-espi)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  environment           show environmental information
  file                  Display filesystem information
  firewall               Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  mac-name             Displays the configured MAC names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                 Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  role                   Configure role parameters
  redundancy             Display redundancy group parameters

  rtls                  Real Time Locating System commands
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration
parameters
  timezone              Display timezone
  traffic-shape        Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently
logged                          in users
  version               Display software & hardware version
```

```
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFSwitch(config-rtls-espi)#show

RFSwitch(config-rtls-espi)#show rtls espi ?
  adapter     Adapter Configuration
  ecspecs     ECSpecs configuration
  subscriber  Show info for giver subsriber's IP
  tags        Tags/Assets (passive, active, wi-fi, uwb)
Information

RFSwitch(config-rtls-espi)#show rtls espi
```

23

RFID Instance

The `(config-rtls-rfid)` instance is used to configure RFID reader related configuration parameters.

To navigate to this instance, use the commands

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#rfid
RFSwitch(config-rtls-rfid)#
```

23.1 RFID Config Commands

Table 23.1 summarizes **`config-rtls-rfid`** commands:

Table 23.1 RFID Config Commands

Command	Description	Ref.
activate	Activates/enables RFID reader configuration	*page 23-3*
clrscr	Clears the display screen	*page 23-4*
end	Ends the current mode and moves to EXEC mode	*page 23-5*
exit	Ends current mode and moves to the previous mode	*page 23-6*
help	Description of the interactive help system	*page 23-7*
no	Negates a command or set its defaults	*page 23-8*
reader	RFID Readers configuration commands	*page 23-9*

Table 23.1 RFID Config Commands

Command	Description	Ref.
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 23-12*
show	Displays the running system information	*page 23-15*

23.1.1 activate

RFID Instance

Activates and enables the *Real Time Location System* (RTLS) adapter

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`activate`

Parameters

None

Usage Guidelines

Use [no] to disable and deactivate the RTLS adapter

Example

```
RFSwitch(config-rtls-rfid)#activate
RFSwitch(config-rtls-rfid)#
```

23.1.2 clrscr

RFID Instance

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-rtls-rfid)#clrscr
RFSwitch(config-rtls-rfid)#
```

23.1.3 end

RFID Instance

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-rtls-rfid)#end
RFSwitch#
```

23.1.4 exit

RFID Instance

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-rtls-rfid)#exit
RFSwitch(config-rtls)#
```

23.1.5 help

RFID Instance

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-rtls-rfid)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-rtls-rfid)#
```

23.1.6 no

RFID Instance

Supported in the following platforms:Negates a RTLS command or set its defaults

- RFS7000
- RFS6000

Syntax

```
no [activate|reader|service]
```

Parameters

activate	Deactivates/disables RTLS adapter
reader	Disables RFID reader configuration commands
service	Disables service commands

Usage Guidelines

Use `[no]` command to undo the configurations on the parameters mentioned in the table. Refer to the parameters, within this chapter, for complete syntax.

Example

```
RFSwitch(config-rtls-rfid)#no activate
RFSwitch(config-rtls-rfid)#
```

23.1.7 reader

RFID Instance

Configures RFID Readers parameters

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
reader [<index>|<reader-index-list>]

reader <index> [antenna|coordinates|description|
  enable|id|name]
reader <index> antenna [<antenna>|<antenna-list>]
reader <index> antenna <antenna-list> [coordinates x
  <x-coordinate> y <y-coordinate> z <z-coordinate>|
  power <antenna-power>]
reader <index> coordinates x <x-coordinate> y <y-coordinate>
  z <z-coordinate>
reader [<index>|<reader-index-list>] id <ip>
reader [<index>|<reader-index-list>] description
  <description>
reader [<index>|<reader-index-list>] enable
reader [<index>|<reader-index-list>] name <name>
```

Parameters

reader [<index>| <reader-index-list>]	Enter a single RFID reader index or a list (1,3,7) or range (3-7) of RFID reader indices

antenna [<antenna>|<antenna-list>] coordinates x <x-coordinate> y <y-coordinate> *z <z-coordinate>*	Configures the RFID readers antenna. Select a antenna using its index, between <1-8> or range (eg:3-7) of antenna indices or any RFID reader antenna • coordinates - Sets the coordinates for the antenna • x <x-coordinate> – Configures the x coordinate for the antenna for the RFID reader. • y <y-coordinate> – Configures the y coordinate for the antenna for the RFID reader. • z <z-coordinate> – Configures the z coordinate for the antenna for the RFID reader.
reader [<index>|<reader-index-list>] antenna [<antenna>|<antenna-list>] power <antenna-power>	Configures the RFID reader power. • power – Sets the power • <antenna-power> – Sets the antenna power to between <-63 and 63 dBm.
reader <index> id <ip>	Sets the IP address <ip> for the reader with index <index>.
reader <index> coordinates x <x-coordinate> y <y-coordinate> *z <z-coordinate>*	Sets the coordinates for the RFID reader. • coordinates - Sets the coordinates for the reader • x <x-coordinate> – Configures the x coordinate for the RFID reader. • y <y-coordinate> – Configures the y coordinate for the RFID reader. • z <z-coordinate> – Configures the z coordinate for the RFID reader.
reader [<index>|<reader-index-list>] description <description>	Sets the description of a RFID reader or a list of readers to <description> (1-32 characters).
reader [<index>|<reader-index-list>] enable	Enables or connects the RFID reader with the index <index> or a list of RFID readers <reader-index-list>.

reader [<index>|<reader-index-list>] name <name>	Sets a user friendly name to a RFID reader or a group of RFID readers to <name> (1-20 characters).

Usage Guidelines

Use `[no] reader [<index>|<range>][options]` to rollback any configurations performed using the `reader` command

Example

```
RFSwitch(config-rtls-rfid)#reader 1 antenna 1 coordinates x
400 y 400 z 500
RFSwitch(config-rtls-rfid)#
```

23.1.8 service

RFID Instance

Invokes service commands to troubleshoot or debug (config-if) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
service reader [<reader-index>|<reader-index-list>]
[antenna|upgrade]

service reader [<reader-index>|<reader-index-list>] antenna
[<antenna-index>|<antenna-list>|any] filter [<tag-filter-
index>|<tag-filter-name>]

service reader [<reader-index>|<reader-index-list>] upgrade
ipaddr <ftp-ip> ftp-username <ftp-username> ftp-password
<ftp-password> ftp-path <file-path> username <reader-admin-
username> password <reader-admin-password>
```

Parameters

show cli	Displays the CLI tree of the current mode

service reader [<reader-index>|<reader-index-list>] antenna [<antenna-index>|<antenna-list>|any] filter [<tag-filter-index>|<tag-filter-name>]	Displays the RFID reader configuration information. • <reader-index> – The RFID reader index. • <reader-index-list> – A list of comma separated RFID reader indices. • antenna [<antenna-index>|<antenna-list>|all] – The antenna information. • <antenna-index> – The antenna index in case of readers with multiple antennae. • <antenna-list> – The list of comma separated antenna indices. • any – Indicates all antennas. • filter [<tag-filter-index>|<tag-filter-name>] – RFID Tag filter configuration • <tag-filter-index> – The index of the Tag Filter. • <tag-filter-name> – The name of the Tag Filter.
service reader [<reader-index>|<reader-index-list>] upgrade ipaddr <ftp-ip> ftp-username <ftp-username> ftp-password <ftp-password> ftp-path <file-path> username <reader-admin-username> password <reader-administrative-password>	Upgrades the RFID readers. • <reader-index> – The RFID reader index. • <reader-index-list> – A list of comma separated RFID reader indices. • upgrade ipaddr <ftp-ip> – Upgrades the selected RFID reader/readers from the ip address <ftp-ip> • ftp-username <ftp-username> – The ftp username for the upgrade FTP server. • ftp-password <ftp-password> – The password for the ftp-username <ftp-username>. • ftp-path <file-path> – The path to the upgrade file on the FTP server. • username <reader-admin-username> – The administrative username on the reader. • password <reader-admin-password> – The password for the username <reader-admin-username>.

Example

```
RFSwitch(config-rtls-rfid)#service show cli
RFID readers Config mode:
+-activate [activate]
+-adopt-unconf-readers [adopt-unconf-readers]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-activate [no activate]
  +-adopt-unconf-readers [no adopt-unconf-readers]
  +-reader
    +-<1-48>
      +-antenna
        +-<1-8>
          +-coordinates [no reader (<1-48>|READER) antenna
(<1-8>|ANTENNA) coordinates]
          +-filter [no reader (<1-48>|READER) antenna (<1-
.....................................................
...
.....................................................
...
.....................................................
...
.....................................................
...
RFSwitch(config-rtls-rfid)#
```

23.1.9 show

RFID Instance

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-rtls-rfid)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
```

```
  dpd                    wios dataplane
  environment            show environmental information
  file                   Display filesystem information
  firewall               Wireless firewall
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and
buffer
  mac                    Internet Protocol (IP)
  mac-address-table      Display MAC address table
  mac-name               Displays the configured MAC names
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port                   Physical/Aggregate port interface
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy-group       Display redundancy group parameters
  redundancy-history     Display state transition history of
the                          switch.
  redundancy-members     Display redundancy group members in
detail
  role                   Configure role parameters
  rtls                   Real Time Locating System commands
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open
connections
  smtp-connections       Display SNMP engine parameters
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration
parameters
  timezone               Display timezone
  traffic-shape          Display traffic shaping
  upgrade-status         Display last image upgrade status
```

```
  users                  Display information about currently
logged                          in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

RFSwitch(config-rtls-rfid)#show

RFSwitch(config-rtls-rfid)#show rtls rfid ?
  LLRP       Reader protocol statistics (LLRP)
  inventory  RFID Tag Inventory
  reader     RFID Reader configuration commands
RFSwitch(config-rtls-rfid)#
```

24

SOLE Instance

Use the `(config-rtls-sole)` instance to configure SOLE Location Engine related parameters.

To navigate to this instance, use the commands

```
RFSwitch(config)#rtls
RFSwitch(config-rtls)#sole
RFSwitch(config-rtls-sole)#
```

24.1 SOLE Config Commands

Table 24.1 summarizes `config-rtls-sole` commands:

Table 24.1 Location Engine Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 24-3*
end	Ends the current mode and moves to EXEC mode	*page 24-4*
exit	Ends current mode and moves to the previous mode	*page 24-5*
help	Description of the interactive help system	*page 24-6*
locate	Configures location commands	*page 24-7*
no	Negates a command or set its defaults	*page 24-9*
redundancy	Enables redundancy support across cluster members for SOLE	*page 24-10*

Table 24.1 Location Engine Config Command Summary (Continued)

Command	Description	Ref.
service	Invokes service commands to troubleshoot or debug `(config-rtls)` instance configurations	*page 24-11*
show	Displays the running system information	*page 24-12*
rssi-filter	Filters rssi value in dbm	*page 24-15*
aap-rssi-update-interval	Displays AAP probe packet interval value in seconds	*page 24-16*
mobile-unit	Displays mobile-unit configurations	*page 24-17*

24.1.1 clrscr

SOLE Instance

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-rtls-sole)#clrscr
RFSwitch(config-rtls-sole)#
```

24.1.2 end

SOLE Instance

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

end

Parameters

None

Example

```
RFSwitch(config-rtls-sole)#end
RFSwitch#
```

24.1.3 exit

SOLE Instance

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-rtls-sole)#exit
RFSwitch(config-rtls-sole)#
```

24.1.4 help

SOLE Instance

Displays the interactive help system for RTLS instance

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-rtls-sole)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-rtls-sole)#
```

24.1.5 locate

SOLE Instance

Configures location commands

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
locate [aeroscout|mobile-unit|ekahau]
locate mobile-unit [<MAC-Addr>|enable|interval]
locate ekahau [enable|interval]
```

Parameters

aeroscout [enable|interval <5-3600>	Locates aeroscout tags • enable – Enables on-board aeroscout location engine service • interval <5-3600> – Configures location interval for on-board locationing of aeroscout tags in seconds
mobile-unit [<MAC-Addr>| enable|interva <5-3600>l]	Locates specified mobile unit • <MAC-Addr> enable – Enables location of specified MU • enable – Enables location of all specified MUs • interval <5-3600> – Configures MUs location interval for locationing of MUs in seconds **Note:** The switch currently supports locationing of 512 MUs only.
ekahau [enable| interval<5-3600>	Locates ekahau tags • enable – Enables on-board locationing of`ekahau` tags • interval <5-3600> – Configures location interval for on-board locationing of ekahau tags in seconds

Usage Guidelines

Use `[no] locate [aeroscout|mobile-unit|ekahau]` to rollback and disable all the configurations performed using `locate` command

Example

```
RFSwitch(config-rtls-sole)#locate aeroscout enable
RFSwitch(config-rtls-sole)#

RFSwitch(config-rtls-sole)#locate aeroscout interval 300
RFSwitch(config-rtls-sole)#
```

24.1.6 no

SOLE Instance

Disables the locationing adapter(s) and its configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [aap-rssi-update-interval|locate|mobile-nit|redundancy|
rssi-filter]
```

Parameters

aap-rssi-update-interval	Disables AAP probe packet interval
locate [aeroscout|ekahau|mobile-unit]	Negates Location commands
mobile-unit [<MAC-Addr|enable|interval <5-3600>]	Locates specified mobile-unit • <MAC-Addr> (enable) – Disables location of specified mobile uit • enable – Disables location of all specified mobile units • interval <5-3600> – Resets the location interval for the locationing of MUs
redundancy enable	Disables SOLE redundancy
rssi-filter	Disables rssi-filter value in dbm

Example

```
RFswitch(config-rtls-sole)#no locate mobile-unit enable
RFswitch(config-rtls-sole)#

RFswitch(config-rtls-sole)#no locate mobile-unit interval
RFswitch(config-rtls-sole)#
```

24.1.7 redundancy

SOLE Instance

Enables redundancy support across cluster members for SOLE

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
redundancy enable
```

Parameterse

redundancy enable	Enables the redundancy support across cluster members for SOLE

Usage Guidelines

This command is disabled by default

Example

```
RFSwitch(config-rtls-sole)#redundancy enable
RFSwitch(config-rtls-sole)#
```

24.1.8 service

SOLE Instance

Invokes service commands to troubleshoot or debug (`config-rtls`) instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-rtls-sole)#service show cli
Location Engine Config mode:
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-locate
  +-aeroscout
    +-enable [locate (aeroscout|ekahau) (interval <5-
3600>|enable)]
    +-interval
      +-<5-3600> [locate (aeroscout|ekahau) (interval <5-
3600>|enable)]
  +-mobile-unit
    +-AA-BB-CC-DD-EE-FF
      +-enable [locate mobile-unit (AA-BB-CC-DD-EE-FF|)
enable]
    +-enable [locate mobile-unit (AA-BB-CC-DD-EE-FF|)
enable]
    +-interval
      +-<5-3600> [locate mobile-unit interval <5-3600>]
  +-ekahau
    +-enable [locate (aeroscout|ekahau) (interval <5-
3600>|enable)]
    +-interval.....................
RFSwitch(config-rtls-sole)#
```

24.1.9 show

SOLE Instance

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000:

- port-channel
- static-channel-group

Syntax

```
show <parameters>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-rtls-sole)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
```

```
  dhcp                    DHCP Server Configuration
  environment             show environmental information
  file                    Display filesystem information
  firewall                Wireless firewall
  ftp                     Display FTP Server configuration
  history                 Display the session command history
  interfaces              Interface status
  ip                      Internet Protocol (IP)
  ldap                    LDAP server
  licenses                Show any installed licenses
  logging                 Show logging configuration and
buffer
  mac                     Internet Protocol (IP)
  mac-address-table       Display MAC address table
  management              Display L3 Managment Interface name
  mobility                Display Mobility parameters
  ntp                     Network time protocol
  password-encryption     password encryption
  port                    Physical/Aggregate port interface
  port-channel            Portchannel commands
  privilege               Show current privilege level
  radius                  RADIUS configuration commands
  redundancy     Display redundancy group parameters

  role                    Configure role parameters
  rtls                    Real Time Locating System commands
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open
connections
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group    static channel group membership
  terminal                Display terminal configuration
parameters
  timezone                Display timezone
  traffic-shape           Display traffic shaping
  upgrade-status          Display last image upgrade status
  users                   Display information about currently
logged                           in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl
```

```
RFSwitch(config-rtls-sole)#show

RFSwitch(config-rtls-sole)#show rtls sole ?
  peers   Show SOLE peer information
  probes  Show probe information
RFSwitch(config-rtls-sole)#

RFSwitch(config-rtls-sole)#show rtls sole peers
SOLE-WCCP status    :DOWN
SOLE-WCCP IP address:0.0.0.0
SOLE-Peer count     :0
RFSwitch(config-rtls-sole)#

RFSwitch(config-rtls-sole)#show rtls sole probes
  #    Tag MAC             Type         Switch-Id  Probes
Time
RFSwitch(config-rtls-sole)#
```

24.1.10 rssi-filter

SOLE Instance

Filters rssi values below this threshold

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
rssi-filter <-100-0>
```

Parameters

<-100-0>	Displays rssi filter value in dbm

Example

```
RFSwitch(config-rtls-sole)#rssi-filter -9
RFSwitch(config-rtls-sole)#
```

24.1.11 aap-rssi-update-interval

SOLE Instance

Displays AAP probe packet interval value in seconds

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
aap-rssi-update-interval <5-3600>
```

Parameters

aap-rssi-update-interval <5-3600>	Displays aap-rssi filter value in seconds

Example

```
RFSwitch(config-rtls-sole)#aap-rssi-update-interval 99
RFSwitch(config-rtls-sole)#
```

24.1.12 mobile-unit

SOLE Instance

Displays mobile-unit configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
mobile-unit power-level <1-100>
```

Parameters

mobile-unit powerlevel <1-100>]	Displays mobile-unit configurations • power-level <1-100> – Displays mobile-unit power-level

Example

```
RFSwitch(config-rtls-sole)#mobile-unit powerlevel 9
RFSwitch(config-rtls-sole)#
```

25

Smart RF Instance

Use the `(config-wireless-smart-rf)` instance to configure Smart RF related configuration commands. To navigate to the `config-wireless-smart-rf` instance, use the following commands:

```
RFSwitch(config)#wireless
RFSwitch(config-wireless)#smart-rf
RFSwitch(config-wireless-smart-rf)#
```

25.1 smart-rf Config Commands

The following table summarizes **`config-wireless-smart-rf`** commands:

Command	*Description*	*Ref.*
assignable-power-range	Specifies the power range during power-assignment	*page 25-3*
auto-assign	Enables individual RF parameters to be auto-assigned	*page 25-4*
clrscr	Clears the display screen	*page 25-5*
end	Ends the current mode and moves to the PRIV EXEC mode	*page 25-6*
exit	Ends the current mode and moves to the previous mode	*page 25-7*
extensive-scan	Enables the extensive-scan mode, calibrations to be made at every tx-power level	*page 25-8*

Command	Description	Ref.
help	Displays the interactive help system	*page 25-9*
hold-time	The number of seconds to disable interference avoidance after a detection	*page 25-10*
no	Negates commands or resets values to default	*page 25-11*
number-of-rescuers	Sets the number of rescuers to cover for faulty radios	*page 25-18*
radio	Smart RF radio related commands	*page 25-19*
recover	Enables individual self-recovery features	*page 25-24*
retry-threshold	Sets the average number of retries before a channel scan is performed	*page 25-25*
run-calibrate	Starts a new automatic RF calibration process	*page 25-26*
scan-dwell-time	Sets the time duration to dwell on a channel during channel scan	*page 25-27*
schedule-calibrate	Sets the parameters for auto-calibrate	*page 25-28*
select-channels	Selects channels for automatic channel scan and Smart RF	*page 25-29*
service	Service commands that sets Smart RF parameters	*page 25-30*
show	Shows the running Smart RF information	*page 25-34*
smart-rf-module	Enables the Smart RF module	*page 25-40*
verbose	Enables the verbose mode that records every Smart RF assignment	*page 25-41*

25.1.1 assignable-power-range

Smart RF Instance

Specifies the power range during power assignment.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`assignable-power-range [<lower bound> <upper bound>]`

Parameters

assignable-power-range [<lower bound> <upper bound>]	Specifies the power range during power assignment. • lower bound – The lower bound of the power range. Value is between 4 and 20. • Upper bound – The upper bound of the power range. Value is between 4 and 20.

Example

```
RFSwitch(config-wireless-smart-rf)#assignable-power-range 4
10
RFSwitch(config-wireless-smart-rf)#
```

25.1.2 auto-assign

Smart RF Instance

Enables individual RF parameters to be auto-assigned

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
auto-assign [all|channel|detector|power|rescuer] enable
```

Parameters

auto-assign [all|channel|detector|power|rescuer] enable	Enables individual RF parameters to be auto-assigned. • all - Enables auto-assign for all the RF parameters • channel enable - Enables auto-assign for channels • detector enable - Enables auto-assign for detectors • power enable - Enables auto-assign for power • rescuer enable - Enables auto-assign for rescuer

Example

```
RFSSwitch(config-wireless-smart-rf)#auto-assign all enable
RFSSwitch(config-wireless-smart-rf)#auto-assign channel
enable
RFSSwitch(config-wireless-smart-rf)#auto-assign detector
enable
RFSSwitch(config-wireless-smart-rf)#auto-assign power enable
RFSSwitch(config-wireless-smart-rf)#auto-assign rescuer
enable
```

25.1.3 clrscr

Smart RF Instance

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`clrscr`

Parameters

None

Example

```
RFSwitch(config-wireless-smart-rf)#clrscr
RFSwitch(config-wireless-smart-rf)#
```

25.1.4 end

Smart RF Instance

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-wireless-smart-rf)#end
RFSwitch#
```

25.1.5 exit

Smart RF Instance

Ends the current mode and moves to the previous mode (`config-wireless`). The prompt changes to `RFSwitch(config-wireless)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-wireless-smart-rf)#exit
RFSwitch(config-wireless)#
```

25.1.6 extensive-scan

Smart RF Instance

Enters the extensive scan mode

The device needs calibration at every `tx-power` level.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
extensive-scan enable
```

Parameters

extensive enable	Enables the extensive scan mode.

Example

```
RFSwitch(config-wireless-smart-rf)#extensive-scan enable
RFSwitch(config-wireless-smart-rf)#
```

25.1.7 help

Smart RF Instance

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFS7000(config-wireless-smart-rf)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-wireless-smart-rf)#
```

25.1.8 hold-time

Smart RF Instance

Defines the number of seconds to disable interference avoidance after a detection

This prevents a radio from changing channels continuously.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`hold-time <30-65535>`

Parameters

hold-time *<30-65535>*	The number of seconds to disable interface avoidance after a detection. This prevents the radio from changing channels continuously. Set the values in seconds from 30-65535.

Example

```
RFSwitch(config-wireless-smart-rf)#hold-time 400
RFSwitch(config-wireless-smart-rf)#
```

25.1.9 no

Smart RF Instance

Disables the Smart RF configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
no [assignable-power-range|auto-assign|extensive-scan|
hold-time|number-of-rescuers|radio|recover|
retry-threshold|scan-dwell-time|schedule-calibrate|
select-channels|service|smart-rf-module|verbose]

no assignable-power-range [<4-20> <4-20>]

no auto-assign [all|channel|detector|power|rescuer]

no extensive-scan enable

no number-of-rescuers

no radio [<1-4096>|MAC-ADDRESS|RADIO|all-11a|all-11b|
all-11bg]

no recover [coverage-hole|interference|neighbor] enable

no retry-threshold [<0.0-15.0>]
no scan-dwell-time [<1-10>]
no schedule-calibrate [enable|interval|start-time]
no select-channels <WORD>
no service smart-rf [max-history|replay enable|rescue]
no smart-rf-module enable
no verbose
```

Parameters

assignable-power-*range* *<4-20> <4-20>*	Negates the power range assignment.

auto-assign [all |channel |detector|power|rescuer] enable	Negates the auto-assign commands • all - Disables all auto-assignment features • channel enable – Disables channel assignments • detector enable – Disables detector assignments • power enable – Disables power assignments • rescuer enable – Disables rescuer assignments
extensive-scan enable	Disables the extensive scan mode
hold-time *<30-65535>*	Disables hold-time for interference avoidance. Set the value in seconds from 30-65535.
number-of-rescuers	Reverts to the default number of rescuers to cover faulty radio

radio [*<1-4096>*| *MAC- Address*|*RADIO*| all-11a|all-11b|all-11bg]	Negates all radio related commands. • *<1-4096>* – For each of the radio, the following values are negated or reset: • antenna-gain <GAIN> – Resets the set antenna gain value. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value. • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value. • radio-mac [AA-BB-CC-DD-EE-FF] – Resets the selected Radio MAC address • rescuer [AA-BB-CC-DD-EE-FF | all] – Resets the selected rescuer MAC address or resets all the rescuers. • *AA-BB-CC-DD-EE-FF* – For the selected Radio MAC, the following parameters are negated or reset. • antenna-gain <GAIN> – Resets the set antenna gain value. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] - Resets the selected coverage rate value. • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value. • *RADIO* – A list of radio index values such as *1,3,5* or *3-7* the following parameter values are negated or reset

radio [*<1-4096>*|*MAC Address*|*RADIO*| all-11a|all-11b|all-11bg] (contd....)	• all-11a - for all 802.11a radios, the following values are negated or reset: • antenna-gain <GAIN> – Resets the set antenna gain value. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54)]- Resets the selected coverage rate value. • lock-auto-assign [all | channel | detector | power | rescuer] - Resets the lock auto assign value. • all-11b - for all 802.11b radios, the following values are negated or reset: • antenna-gain <GAIN> – Resets the set antenna gain value. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value. • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value. • all-11bg - for all 802.11bg radios, the following values are negated or reset: • antenna-gain <GAIN> – Resets the set antenna gain value. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Resets the selected coverage rate value. • lock-auto-assign [all | channel | detector | power | rescuer] – Resets the lock auto assign value.
recover [coverage-hole| interference|neighbor] enable	Negates recover commands. • coverage-hole enable – Negates the command to recover from coverage-hole. • interference enable – Negates the command to recover from interference. • neighbor enable – Negates the command to recover from faulty neighbor radio condition.
retry-threshold [*<0.0-15.0>*]	Resets recovery-threshold values to default.

scan-dwell-time *<1-10>*	Resets the time a scan dwells on a channel during scan.
schedule-calibrate [enable|interval| start-time]	Resets the calibration schedule parameters. • enable – Disables the calibration schedule feature. • interval – Negates the calibration schedule interval. • start-time – Negates the calibration schedule start time.
service smart-rf [max-history|replay (enable)|rescue]	Resets the Smart RF related service commands. • smart-rf max-history – Resets the maximum number history entries. • replay enable – Disables the replay mode. • rescue <WORD> – Removes rescue operation • WORD – A single radio MAC address
select-channels <WORD>	Revert selected- channels to default • WORD– A comma-separated list of channels
smart-rf-module enable	Disables the feature
verbose enable	Disables the verbose mode of recording every assignment.

Example

```
RFSwitch(config-wireless-smart-rf)#no ?
assignable-power-range  reset the power range to default
auto-assign             disable individual RF parameters to
beauto-assigned
extensive-scan          extensive scan mode, calibrate at
everytx-power level
hold-time               The number of seconds to disable
                        interference avoidance after a
detection.
                        This prevents a radio from changing
                        channels continuously
number-of-rescuers      revert to default the number of
rescuers to cover faulty radio

radio                   Radio related commands
recover                 disable individual self-recovery
features
```

```
retry-threshold         The average number retries to cause
a radio to re-run channel selection

scan-dwell-time         The number of seconds to dwell on a
                        channel during scan
schedule-calibrate      configure calibration schedule
parameters
select-channels         Revert selected-channels to default
service                 Service Commands
smart-rf-module         smart-rf module
verbose                 verbose mode, record every
assignment

RFSwitch(config-wireless-smart-rf)#

RFSwitch(config-wireless-smart-rf)#no assignable-power-range
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no auto-assign all enable
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no extensive-scan enable
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no hold-time 100
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no number-of-rescuers
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no radio 1 antenna-gain
10
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no radio all-11a antenna-
gain 10
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no recover coverage-hole
enable
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no retry-threshold 10.0
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no scan-dwell-time 10
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no schedule-calibrate
enable
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no select-channels
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no service smart-rf max-
history
```

```
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no smart-rf-module enable
RFSwitch(config-wireless-smart-rf)#
RFSwitch(config-wireless-smart-rf)#no verbose enable
RFSwitch(config-wireless-smart-rf)#
```

25.1.10 number-of-rescuers

Smart RF Instance

Configures the number of rescuers to cover faulty radio conditions

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`number-of-rescuers <1-5>`

Parameters

number-of-rescuers *<1-5>*	The number of rescuers to use to cover faulty radio conditions.

Example

```
RFSwitch(config-wireless-smart-rf)#number-of-rescuers 2
RFSwitch(config-wireless-smart-rf)#
```

25.1.11 radio

▸ *Smart RF Instance*

Configures the different Smart RF radio parameters

Supported in the following platforms:

- RFS7000
- RFS6000

```
radio [<1-4096>|MAC-ADDRESS|RADIO|all-11a|all-11b|all-11bg]

radio <1-4096> [antenna-gain|coverage-rate|
lock-auto-assign | radio-mac | rescuer]
radio <1-4096> anternna-gain <GAIN>
radio <1-4096> coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio <1-4096> lock-auto-assign
[all|channel|detector|power|rescuer]
radio <1-4096> radio-mac [MAC-ADDRESS]
radio <1-4096> rescuer [MAC-ADDRESS <4-20> <0-65535>]

radio MAC-ADDRESS anternna-gain <GAIN>

radio MAC-ADDRESS coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio MAC-ADDRESS lock-auto-assign
[all|channel|detector|power|rescuer]

radio RADIO anternna-gain <GAIN>
radio RADIO coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio RADIO lock-auto-assign
[all|channel|detector|power|rescuer]

radio all-11a anternna-gain <GAIN>

radio all-11a coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11a lock-auto-assign
[all|channel|detector|power|rescuer]

radio all-11b anternna-gain <GAIN>
```

```
radio all-11b coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11b lock-auto-assign
[all|channel|detector|power|rescuer]

radio all-11bg anternna-gain <GAIN>

radio all-11bg coverage-rate
[1|2|5p5|6|9|11|12|18|24|36|48|54]
radio all-11bg lock-auto-assign
[all|channel|detector|power|rescuer]
```

Parameters

<1-4096>[antenna-gain | coverage-rate | lock-auto-assign | radio-mac | rescuer]	Sets the following parameters for the selected radio: • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments. • radio-mac <AA-BB-CC-DD-EE-FF> – Sets the radio MAC address for the radio with the selected index. • rescuer {AA-BB-CC-DD-EE-FF *<4-20>* *<0-65535>*} – Sets the MAC address for the rescuer radio. The following parameters are also set: • *<4-20>* – Boost power to cover for the defective radio. • *<0-65535>* – Attenuation from the rescuer radio to the selected radio. This is for information purposes only.

AA-BB-CC-DD-EE-FF [antenna-gain | coverage-rate | lock-auto-assign | rescuer]	Sets the following parameters for the selected radio. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments. • rescuer {AA-BB-CC-DD-EE-FF *<4-20>* *<0-65535>* }– Sets the MAC address for the rescuer radio. The following parameters are also set: • *<4-20>* – Boost power to cover for the defective radio. • *<0-65535>* – Attenuation from the rescuer radio to the selected radio. This is for information purposes only.
RADIO [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters to a set of radio indices. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.

all-11a [antenna-gain| coverage-rate|lock-auto- assign]	Sets the radio parameters for all 802.11a radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.
all-11b [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters for all 802.11b radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.
all-11bg [antenna-gain| coverage-rate| lock-auto-assign]	Sets the radio parameters for all 802.11bg radios. • antenna-gain <GAIN> – Sets the antenna-gain value to GAIN for the selected radio. • coverage-rate [1|2|5p5|6|9|11|12|18|24|36|48|54] – Sets the coverage rate threshold value for under-coverage detection to the selected value from the list. • lock-auto-assign [all|channel|detector|power|rescuer] – Locks rf configuration from automatic smart rf assignments.

Example

```
RFSwitch(config-wireless-smart-rf)#radio 1 antenna-gain 20
RFSwitch(config-wireless-smart-rf)#radio 1 coverage-area 18
RFSwitch(config-wireless-smart-rf)#radio 1 lock-auto-assign
channel
RFSwitch(config-wireless-smart-rf)#radio 1 radio-mac 1-2-3-
4-5-6
RFSwitch(config-wireless-smart-rf)#radio 1 rescuer 1-2-3-4-
5-6 20 30
RFSwitch(config-wireless-smart-rf)#radio 1-2-3-4-5-6
antenna-gain 20
RFSwitch(config-wireless-smart-rf)#radio 2-5,8,11,15
antenna-gain 20
RFSwitch(config-wireless-smart-rf)#radio all-11a coverage-
rate 5p5
RFSwitch(config-wireless-smart-rf)#radio all-11b lock-auto-
assign power
RFSwitch(config-wireless-smart-rf)#radio all-llbg antenna-
gain 20
RFSwitch(config-wireless-smart-rf)#
```

25.1.12 recover

Smart RF Instance

Enables individual self-recovery features

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
recover [coverage-hole|interference|neighbor]
```

Parameters

recover [coverage-hole| interference|neighbor] enable	Enables individual self recovery features: • coverage-hole enable – Enables recovery from coverage-hole errors • interference enable – Enables recovery from interference errors • neighbor enable – Enables recovery from errors due to faulty neighbor radios

Example

```
RFSwitch(config-wireless-smart-rf)#recover coverage-hole
enable
RFSwitch(config-wireless-smart-rf)#recover interference
enable
RFSwitch(config-wireless-smart-rf)#recover neighbor enable
RFSwitch(config-wireless-smart-rf)#
```

25.1.13 retry-threshold

Smart RF Instance

Sets the threshold for the average number of retries performed before a radio re-runs a channel scan

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`retry-threshold <0.0-15.0>`

Parameters

<0.0-15.0>	The value in decimal number. This is the average number of retries a radio makes before it re-runs the channel scan.

Example

```
RFSwitch(config-wireless-smart-rf)#retry-threshold 8.4
RFSwitch(config-wireless-smart-rf)#
```

25.1.14 run-calibrate

Smart RF Instance

Starts an automatic RF configuration process

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
run-caliberate
```

Parameters

None

Example

```
run-caliberate
```

25.1.15 scan-dwell-time

Smart RF Instance

Sets the time in seconds to dwell on a channel during a channel scan

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`scan-dwell-time <1-10>`

Parameters

scan-dwell-time <1-10>	The duration in seconds to dwell on a channel during a channel scan.

Example

```
RFSwitch(config-wireless-smart-rf)#scan-dwell-time 10
RFSwitch(config-wireless-smart-rf)#
```

25.1.16 schedule-calibrate

Smart RF Instance

Configures the calibrate schedule parameters

This is used to configure parameters that schedule the automatic configuration of the Smart RF feature.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
schedule-calibrate [enable |interval |start-time]
schedule-calibrate interval <1-366>
schedule-calibrate start-time <HH:MM> <1-31> <1-12>
<2008-2035>
```

Parameters

enable	Enables the schedule-calibrate feature. When enabled, the Smart RF auto calibration feature is performed at the set interval.
interval *<1-366>*	Sets the interval in days between each auto calibration.
start-time *<HH:MM>* *<1-31>* *<1-12>* <2008-2035>	Sets the time and day to start the first auto-calibration. <HH:MM> is in 24 hours format.

Example

```
RFSwitch(config-wireless-smart-rf)#schedule-calibrate enable
RFSwitch(config-wireless-smart-rf)#schedule-calibrate
interval 2
RFSwitch(config-wireless-smart-rf)#schedule-calibrate
                                    start-time 10:30 1 1
RFSwitch(config-wireless-smart-rf)#
```

25.1.17 select-channels

Smart RF Instance

Selects a list of channels for Automatic Channel Scan and Smart RF

Use this command to add channels or remove them from the channel list.

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
select-channel [<WORD>|add<WORD>|remove <WORD>]
```

Parameters

<WORD>	A comma separated list of channel numbers.
add <WORD>)	Add a channel or a list of channels to the channel list.
remove <WORD>	Remove a channel or a list of channels from the channel list

Example

```
RFSwitch(config-wireless-smart-rf)#select-channels 1,2,15-17
RFSwitch(config-wireless-smart-rf)#select-channels add
1,2,15-17
RFSwitch(config-wireless-smart-rf)#select-channels remove
1,2,15-17
RFSwitch(config-wireless-smart-rf)#
```

25.1.18 service

Smart RF Instance

Invokes service commands to troubleshoot or debug `(config-wireless-smart-rf)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
service smart-rf [clear-history|load-from-file|max-history
|replay|rescue|restore|save-to-file|simulate|step-calibrate]

service smart-rf clear-history
service smart-rf load-from-file
service smart-rf max-history <0-65535>
service smart-rf replay enable
service smart-rf rescue <WORD>
service smart-rf restore [WORD]
service smart-rf save-to-file
service smart-rf simulate [coverage-hole <1-4096> UINT_RANGE
{UINT_RANGE|pattern-11a|pattern-11b|
pattern-11bg|pattern-2-mbps}|interference]

service smart-rf simulate interference <WORD>

service smart-rf step-calibrate [assign-channel|
assign-detectors|assign-power|assign-prepare|
assign-rescuers|collect-data|prepare-detectors|
pull-rf-config|push-rf-config|sync-rf-config]
```

Parameters

show cli	Displays the CLI tree of the current mode.
smart-rf [clear-history | load-from-file| max-history|replay| rescue|restore| save-to-file|simulate| step-calibrate]	Smart RF related commands are executed from this service command. • clear-history – Clears assignment history • load-from-file – Loads Smart RF record from file *smart.bin* • max-history *<0-65535>* – Sets the number of assignment items to be retained as history. • replay enable – Enables the Smart RF replay mode • rescue <WORD> – Enables force rescue operation • restore <WORD> – Removes any recovering operation on given radio • save-to-file – Saves Smart RF records to the local file *smart.bin* • simulate [coverage-hole|interference] – Simulates the different radio events • coverage-hole <UINT_RANGE> – Simulates the coverage-hole event • UINT_RANGE [pattern-11a|pattern-11b |pattern11bg|pattern-2-mbps] – provide simulated MU's allowed • interference – Simulates radio interferences • step-calibrate [assign-channels|assign-detectors| assign-power|assign-prepare|assign-rescuers| collect-data|prepare-detectors|pull-rf-config| push-rf-config|sync-rf-config] – Manages Smart-RF commands • assign-channels – Assigns channels to radios • assign-detectors – Assigns detectors • assign-power – Assigns tx power to radios

	• assign-prepare – Prepares assignment • assign-rescuers – Assigns rescuers along with recovering power • collect-data – Collects site measurement data • prepare-detectors – Prepare prior to assign detectors • pull-rf-config – Pull RF-configuration from cluster members • push-rf-config – Push Rf-configuration to cluster members • sync-rf-config – Sync RF-configuration of cluster members

Example

```
RFSwitch(config-wireless-smart-rf)#service show cli
Smart-RF Configuration mode:
+-assignable-power-range
  +-<4-20>
    +-<4-20> [assignable-power-range <4-20> <4-20>]
+-auto-assign
  +-all
    +-enable [auto-assign
(detector|channel|power|rescuer|all) enable]
  +-channel
    +-enable [auto-assign
(detector|channel|power|rescuer|all) enable]
  +-detector
    +-enable [auto-assign
(detector|channel|power|rescuer|all) enable]
  +-power
    +-enable [auto-assign
(detector|channel|power|rescuer|all) enable]
  +-rescuer
    +-enable [auto-assign
(detector|channel|power|rescuer|all) enable]
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-extensive-scan
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
```

```
+-help [help]
+-hold-time
  +-<30-65535> [hold-time <30-65535>]
+-no
  +-assignable-power-range [no assignable-power-range]
  +-auto-assign
    +-all
      +-enable [no auto-assign
(detector|channel|power|rescuer|all) enable]
    +-channel
      +-enable [no auto-assign
(detector|channel|power|rescuer|all) enable]
    +-detector
      +-enable [no auto-assign
(detector|channel|power|rescuer|all) enable]
    +-power
      +-enable [no auto-assign
(detector|channel|power|rescuer|all) enable]
    +-rescuer
      +-enable [no auto-assign
(detector|channel|power|rescuer|all) enable]
  +-extensive-scan
    +-enable [no (smart-rf-module|verbose|extensive-scan)
enable]
  +-hold-time [no hold-time (|<30-65535>)]
    +-<30-65535> [no hold-time (|<30-65535>)]
  +-number-of-rescuers [no number-of-rescuers]


.....


+-smart-rf-module
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
+-verbose
  +-enable [(smart-rf-module|verbose|extensive-scan) enable]
+-write
  +-memory [write memory]
```

25.1.19 show

Smart RF Instance

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000 :

- port-channel
- static-channel-group

Syntax

```
show <parameters>
show wireless smart-rf [calibration-status|configuration|
history |radio]
show wireless smart-rf calibration-status
show wireless smart-rf configuration
show wireless smart-rf history

show wireless smart-rf radio [config|local-status|map|
master-status|neighbors|spectrum]

show wireless smart-rf radio config[<1-4096>|MAC_ADDRESS
|all-11a|all-11bg]

show wireless smart-rf radio local-status[<1-4096>|
MAC_ADDRESS|all-11a|all-11bg]

show wireless smart-rf radio map [MAC_ADDRESS|all-11a|
all-11bg]
show wireless smart-rf radio master-status [MAC_ADDRESS|
all-11a|all-11bg]
show wireless smart-rf radio neighbors [MAC_ADDRESS|
all-11a|all-11bg]
show wireless smart-rf radio spectrum [MAC_ADDRESS|
all-11a|all-11bg]
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-wireless-smart-rf)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  firewall             Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                   Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy     Display redundancy group parameters
```

```
  role                    Configure role parameters
  rtls                    Real Time Locating System commands
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open
connections
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group    static channel group membership
  terminal                Display terminal configuration
parameters
  timezone                Display timezone
  traffic-shape           Display traffic shaping
  upgrade-status          Display last image upgrade status
  users                   Display information about currently
logged                          in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl

RFSwitch(config-wireless-smart-rf)#show wireless ? aap-
version                   The minimum Adaptive firmware
version string
  ap                            Status of adopted access-port
  ap-containment                Rogue AP Containment
  ap-detection-config           Detected-AP Configuration
Parameters
  ap-images                     List of access-port images on
the
                              wireless switch
  ap-unadopted                  List of unadopted access-port
  approved-aps                  Approved APs seen by access-
port
                              scans
  channel-power                 List of available channel and
power
                              levels for a radio
  client                        wireless client configuration
  config                        Wireless Configuration
Parameters
  country-code-list             List of supported country
names and 2
                              letter IS0 3166 codes
```

```
  default-ap                    Information for default
access-port
  hotspot-config                Wlan hotspot configuration
  ids                           Intrusion detection parameters
  known                         Known AP related parameters
  mac-auth-local                list out the mac-auth-local
entries
  mesh                          Mesh related parameters
  mobile-unit                   Details of associated mobile-
units
  multicast-packet-limit        multicast-packet-limit
  phrase-to-key                 display the WEP keys generated
by a
                              passphrase
  qos-mapping                   Quality of Service mappings
used for
                              mapping wireless priorities and
                              802.1p / DSCP tags
  radio                         Radio related commands
  radio-group                   radio group configuration
  regulatory                    Regulatory (allowed channel/
power)
                              information for a particular
country
  self-heal-config              Self-Healing Configuration
Parameters
  sensor                        Wireless Intrusion Protection
System
                              parameters. Use "sensor vlan x"
to
                              specify the vlan(s) to which the
                              sensors are connected.
  smart-rf                      Smart-RF Management Commands
  unapproved-aps                Unapproved APs seen by access-
port or
                              mobile-unit scans
  wireless-switch-statistics  wireless-switch  statistics
  wlan                          Wireless LAN related
parameters

RFSwitch(config-wireless-smart-rf)#show wireless smart-rf ?
  calibration-status  display smart-rf calibration status
  configuration       display smart-rf configuration
  history             display smart-rf assignment history
since
                    latest calibration
```

```
  radio                Radio related commands
RFSwitch(config-wireless-smart-rf)#
```

```
RFSwitch(config-wireless-smart-rf)#show wireless smart-rf
configuration
Smart-RF Module          : disabled

Smart-RF Calibration configuration:
  auto-assign detector   : enabled
  auto-assign channel    : disabled
  auto-assign power      : enabled
  auto-assign rescuer    : enabled
  channels selected      :
  channels excluded      :
  assignable-power-range : [ 4 - 16 ] dBm
  number of rescuers     : 3
  scan dwell time        : 1 second
  retry-threshold        : 14.0 averaged retries/packet
  hold-time              : 3600 seconds

Smart-RF Calibration Schedule:
  schedule calibration   : disabled
  schedule first-start   : Sat Mar 29 03:30:00 2008
  schedule interval      : 1 day(s)

Smart-RF Run Time Monitor and Recovery configuration:
  recover interference   : enabled
  recover neighbor       : enabled
  recover coverage-hole  : enabled

Diagnostic configuration:
  Verbose Mode           : disabled
  Extensive Scan Mode    : disabled

RFSwitch(config-wireless-smart-rf)#
```

```
RFS7000(config-wireless-smart-rf)#show wireless smart-rf
calibration-status

Smart-RF Calibration is busy at delay-second

Smart Master IP:     0.0.0.0
```

```
My           IP:     0.0.0.0
Cluster Master :     yes

Last Calibration Started at: Sun Sep  7 06:01:48 2008
Last Calibration Ended at:   Sun Sep  7 06:01:48 2008
Next calibration Starts at:  not scheduled

RFSwitch(config-wireless-smart-rf)#

RFSwitch(config-wireless-smart-rf)#show wireless smart-rf
history

Smart Master IP:     0.0.0.0
My           IP:     0.0.0.0
Cluster Master :     yes

Last Calibration Started at: Sun Sep  7 06:03:33 2008
Last Calibration Ended at:   Sun Sep  7 06:03:33 2008
Next calibration Starts at:  not scheduled

Smart RF assignment history since last calibration, up to
9216 entries

RFSwitch(config-wireless-smart-rf)#
```

25.1.20 smart-rf-module

Smart RF Instance

Enables the Smart RF feature

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
smart-rf-module enable
```

Parameters

smart-rf-module enable	Enables Smart RF.

Example

```
RFSwitch(config-wireless-smart-rf)#smart-rf-module enable
RFSwitch(config-wireless-smart-rf)#
```

25.1.21 verbose

Smart RF Instance

Enables the verbose mode that records every Smart RF assignment

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
verbose enable
```

Parameters

verbose enable	Enables the verbose mode where every Smart RF assignment is recorded.

Example

```
RFSwitch(config-wireless-smart-rf)#verbose enable
RFSwitch(config-wireless-smart-rf)#
```

26

Role Instance

Use the `(config-role)` instance to configure Role related configuration commands. To navigate to the `config-role` instance, use the following commands:

```
RFSwitch(config)#role <rolename> <rolepriority>
RFSwitch(config-role)#
```

For more information on the `role` command, see *role on page 5-80*.

26.1 Role Config Commands

The following table summarizes **`config-role`** commands:

Command	*Description*	*mRef.*
ap-location	Sets the AP location configuration	*page 26-3*
authentication-type	Sets the authentication type configuration	*page 26-5*
encryption-type	Sets the encryption type	*page 26-6*
essid	Sets ESSID configuration for role based firewall	*page 26-8*
group	Sets role group properties	*page 26-9*
ip	Sets IP configuration properties	*page 26-10*
mac	Sets MAC configuration properties	*page 26-11*

Command	***Description***	***mRef.***
mu-mac	Sets MU MAC configuration properties	*page 26-12*
no	Negates role commands.	*page 26-14*
service	Invokes service commands to troubleshoot or debug `(config-dhcp)` instance configurations	*page 26-18*
show	Displays the running system information	*page 26-19*
clrscr	Clears the display screen	*page 26-13*
exit	Ends the current mode and moves to the previous mode	*page 26-16*
end	Ends the current mode and moves to the EXEC mode	*page 26-15*
help	Displays the interactive help system in HTML format	*page 26-17*

26.1.1 ap-location

Role Config Commands

Sets the AP location configuration

- This requires the location engine to be enabled on the RF Switch with a site, appropriate zones defined and AP co-ordinates defined. The role based firewall has to know which zone the MU is located when it associates for the ap-parameter option to work.
- The 'ap-location' parameter defines the zone or zones you wish to match.

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
ap-location [any|contains|exact|not-contains]
ap-location any
ap-location contains <WORD>
ap-location exact <WORD>
ap_location not-contains <WORD>
```

Parameters

any	Defines any AP location.
contains <WORD>	AP location contains the string <WORD>.
exact <WORD>	AP location contains the exact string <WORD>
not-contains <word>	AP location does not contain the string <WORD>

Example

```
RFSwitch(config-role)#ap-location any
RFSwitch(config-role)#

RFSwitch(config-role)#ap-location contains office
RFSwitch(config-role)#


RFSwitch(config-role)#ap-location exact warehouse
RFSwitch(config-role)#
```

```
RFSwitch(config-role)#ap-location not-contains office
RFSwitch(config-role)#
```

26.1.2 authentication-type

Role Config Commands

Selects authentication type for the role

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
authentication-type [any|eq|neq]

authentication-type any

authentication-type eq [eap|hotspot|kerberos|mac-auth|none]

authentication-type neq[eap|hotspot|kerberos|mac-auth|none]
```

Parameters

any	Any type of authentication.
eq [eap|hotspot|kerberos| mac-auth|none]	Authentication type equals one of the following: • eap – Extensible Authentication Protocol • hotspot – Hotspot authentication • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used
neq [eap|hotspot|kerberos| mac-auth|none]	Authentication protocol does not contain one of the listed options.

Example

```
RFSwitch(config-role)#authentication-type any
RFSwitch(config-role)#
```

26.1.3 encryption-type

Role Config Commands

Selects encryption for the role

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
encryption-type [any|eq|neq]

encryption-type any

encryption-type eq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64]

encryption-type neq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64]
```

Parameters

any	Encryption type can be any
eq [ccmp|keyguard|none|tkip|tkip-ccmp| wep128|wep128-keyguard|wep64]	Encryption type equals one of the following: • ccmp • keyguard • none • tkip • tkip-ccmp • wep128 • wep128-keyguard • wep64

neq [ccmp|keyguard|none|tkip|tkip-ccmp| wep128|wep128-keyguard|wep64]	Encryption type must not be one of the listed options.

Example

```
RFSwitch(config-role)#encryption-type wep128
RFSwitch(config-role)#
```

26.1.4 essid

Role Config Commands

Sets ESSID configuration for the role

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
essid [any|contains|exact|not-contains]

essid any
essid contains <WORD>
essid exact <WORD>
essid not-contains <WORD>
```

Parameters

any	Any ESSID.
contains <WORD>	ESSID contains the string <WORD>.
exact <WORD>	ESSID contains the exact string <WORD>
not-contains <word>	ESSID does not contain the string <WORD>

Example

```
RFSwitch(config-role)#essid any
RFSwitch(config-role)#
```

26.1.5 group

Role Config Commands

Sets group configuration for the role

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
group [any|contains|exact|not-contains]
group any
group contains <WORD>
group exact <WORD>
group not-contains <WORD>
```

Parameters

any	Any group.
contains <WORD>	Group contains the string <WORD>.
exact <WORD>	Group contains the exact string <WORD>
not-contains <word>	Group does not contain the string <WORD>

Example

```
RFSwitch(config-role)#group any
RFSwitch(config-role)#
```

26.1.6 ip

Role Config Commands

Sets IP parameters for the role

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
```

Parameters

access-group [<1-99>| <100-199>|<1300-1999>| <2000-2699>|<WORD>] [in|out] acl-precedence <1-100>	Sets the ACL precedence for the following ACL List entries • <1-99> – IP standard access list • <100-199> – IP extended access list • <1300-1999> – IP standard access list (expanded range) • <2000-2699> – IP extended access list (expanded range) • <word> – IP access list name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – Sets ACL precedence to a value between 1 and 100.

Example

```
RFSwitch(config-role)#ip access-group 8 in acl-precedence
RFSwitch(config-role)#
```

26.1.7 mac

Role Config Commands

Sets MAC access group configuration commands

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
mac access-group <WORD> [in|out] acl-precedence <1-100>
```

Parameters

access-group <word> [in|out] acl-precedence <1-100>	Sets MAC access group configuration parameters • <WORD> – The ACL name • in – Apply grouping to incoming packets • out – Apply grouping to outgoing packets • acl-precedence <1-100> – sets ACL precedence to a value between 1 and 100.

Example

```
RFSwitch(config-role)#mac access-group 8 in acl-precedence
RFSwitch(config-role)#
```

26.1.8 mu-mac

Role Config Commands

Configures the MU MAC addresses for role based firewall

Syntax

```
mu-mac [<MAC Address>|<MAC Address>/<Mask>|any]
```

Parameters

<MAC Address>	The address of the MU that is allowed. MAC address can be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF.
<MAC Address>/<Mask>	The address and mask combination for the mu to be allowed. <MAC Address> and <Mask> should be in the format AA:BB:CC:DD:EE:FF or AA-BB-CC-DD-EE-FF or AABB.CCDD.EEFF
any	Match with any MAC address.

Example

```
RFSwitch(config-role)#mu-mac aa:bb:cc:dd:ee:ff
RFSwitch(config-role)#
```

26.1.9 clrscr

Role Config Commands

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
clrscr
```

Parameters

None

Example

```
RFSwitch(config-role)#clrscr
RFSwitch(config-role)#
```

26.1.10 no

Role Config Commands

Negates role commands

Supported in the following platforms:

- RFS6000
- RFS7000

Syntax

```
no [ap-location|authentication-type|encryption-type|essid|
group|ip|mac|mu-mac]

no ap-location
no authentication-type
no encryption-type
no essid
no group
no ip access-group [<1-99>|<100-199>|<1300-1999>|
<2000-2699>|<WORD>] [in|out] acl-precedence <1-100>
no mac <WORD> [in|out] acl-precedence <1-100>
no mu-mac
```

26.1.11 end

Role Config Commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `RFSwitch#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`end`

Parameters

None

Example

```
RFSwitch(config-role)#end
RFSwitch#
```

26.1.12 exit

Role Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFSwitch#(config)#`

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`exit`

Parameters

None

Example

```
RFSwitch(config-role)#exit
RFSwitch(config)#
```

26.1.13 help

Role Config Commands

Displays the system's interactive help in HTML format

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

`help`

Parameters

None

Example

```
RFSwitch(config-role)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must
backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each
possible
   argument.
2. Partial help is provided when an abbreviated argument is
entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFSwitch(config-dhcp)#
```

26.1.14 service

Role Config Commands

Invokes service commands to troubleshoot or debug `(config-role)` instance configurations

Supported in the following platforms:

- RFS7000
- RFS6000

Syntax

```
service show cli
```

Parameters

None

Example

```
RFSwitch(config-role#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-class
  +-WORD [class WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
 +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
.......................
.....................................................
RFSwitch(config-dhcp)#
```

26.1.15 show

Role Config Commands

Displays current system information

Supported in the following platforms:

- RFS7000
- RFS6000



SWITCH NOTE: The following commands display only for RFS6000:

- power

The following commands display only for RFS7000: port-channel

- static-channel-group

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
RFSwitch(config-role)#show ?
  access-list        Internet Protocol (IP) aclstats
Show ACL Statistics information
  alarm-log             Display all alarms currently in the
system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login
banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
```

```
  firewall              Wireless firewall
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and
buffer
  mac                   Internet Protocol (IP)
mac-address-table     Display MAC address table
  mac-name              Displays the configured mac names
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port                  Physical/Aggregate port interface
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy      Display redundancy group parameters
  rtls                  Real Time Locating System commands
  role                  Configure role parameters
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open
connections
  smtp-notification     Display SNMP engine parameters
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration
parameters
  timezone              Display timezone
  traffic-shape         Display traffic shaping
  upgrade-status        Display last image upgrade status
  users                 Display information about currently
logged                          in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFSwitch(config-role)#
```

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-121710-01 Revision A
March 2009